Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Groupe de coordination interdépartemental politique numérique de l'UE (GI-PNEU)

Berne, le 13.02.2025

La Suisse et la politique numérique de l'Union européenne

Analyse réalisée par le Groupe de coordination interdépartemental politique numérique de l'UE (GI-PNEU)

Etat au: 18.12.2024

Au sujet du document

Le présent document d'analyse a été établi par le Groupe de coordination interdépartemental de la Confédération "Politique numérique UE", chargé d'assurer un suivi de la stratégie numérique de l'UE et d'informer régulièrement le Conseil fédéral des nouveaux développements. Tous les deux ans, ce groupe élabore, sous la coordination de l'OFCOM et du DFAE (Secrétariat d'Etat, Division Europe) une analyse détaillée des évolutions de la réglementation liées à la politique numérique de l'UE.

La stratégie numérique de l'UE comporte aujourd'hui 33 mesures. Le présent document en donne un aperçu et analyse leurs éventuelles conséquences pour la Suisse. Certaines d'entre elles ont été communiquées dès le début du mandat de la nouvelle Commission, dirigée par Ursula von der Leyen, et sont aujourd'hui achevées, d'autres ont été ajoutées plus tard et sont toujours en cours de mise en œuvre. La stratégie est donc à la fois vaste et hétérogène.

Le présent document est un instantané. Les mesures examinées se trouvent à différents stades et peuvent avoir des répercussions différentes selon la pratique de mise en œuvre et d'application. Ce document et les analyses qu'il contient doivent donc être pris avec la prudence qui s'impose.

Table des matières

Executive Summary

La Commission von der Leyen I a été particulièrement active dans le domaine de la politique numérique au cours de la dernière législature (2019-2024). La Commission européenne a lancé 59 mesures législatives depuis 2020 et en a mené 44 à bien à ce jour (think tank Bruegel).

L'attractivité du marché intérieur de l'UE, le *timing* des mesures de régulation et l'influence de la Commission européenne en tant qu'autorité de régulation et de mise en œuvre permettent à l'UE de définir les normes **et d'exercer une influence réglementaire au niveau mondial**. Par conséquent, la politique numérique de l'UE a également des répercussions sur la Suisse.

Les effets de nombreuses mesures de politique numérique se font sentir au-delà des frontières de l'UE, et donc aussi en Suisse et au niveau des entreprises suisses actives sur le marché de l'UE. C'est là le résultat direct des efforts déployés par l'UE pour préserver l'intégrité et l'ordre juridique du marché intérieur européen dans l'espace numérique transfrontalier. Concrètement, il se traduit notamment par l'**utilisation d'instruments de régulation conçus pour appliquer des normes de l'UE à des pays tiers** (p. ex. les procédures d'équivalence et la désignation d'un représentant juridique dans l'UE).

Par ailleurs, ces mesures modifient souvent la structure institutionnelle de l'UE. Une partie non négligeable des nouvelles législations sont des actes juridiques horizontaux et intersectoriels, et impliquent donc souvent un **transfert de compétences** (au moins partiel) des Etats membres vers la Commission européenne. Dans certains domaines, ils représentent un défi également pour la Suisse, qui doit remplacer les canaux établis de coopération réglementaire ou d'échange d'informations.

La présente analyse n'a **pas identifié de risques importants concernant l'accès au marché intérieur** dans le domaine numérique pour les entreprises suisses. Toutefois, certaines mesures, telles que les règlements sur l'intelligence artificielle (mesure 1), sur la cyber-résilience (mesure 16) ou sur l'écoconception (mesure 20), auront des répercussions dans les domaines couverts par l'accord entre la Suisse et l'UE relatif à la reconnaissance mutuelle en matière d'évaluation de la conformité (ARM). De nouvelles exigences viendront s'ajouter à celles qui existent déjà et pourraient, si l'ARM n'est pas étendu aux domaines concernés, constituer pour les entreprises suisses des **obstacles commerciaux supplémentaires**.

Les mesures législatives se trouvent actuellement en grande partie au stade de la mise en œuvre. Cette mise en œuvre, associée aux éventuelles jurisprudences, influencera de manière déterminante le succès des initiatives de politique numérique préconisées par la Commission von der Leyen I, et dans certaines circonstances, la Suisse également.

L'analyse des mesures a montré que l'administration fédérale suit de près les évolutions de la politique numérique et qu'elle est consciente de leurs possibles répercussions. Dans différents domaines, le **Conseil fédéral a déjà agi en conséquence** et pris des mesures en Suisse.

La prochaine analyse complète est prévue pour **le début 2027**.

Mesure 1

Règlement sur l'IA

Appellation complète de la mesure	Règlement établissant des règles harmonisées concernant l'intelligence artificielle
Type de mesure	Règlement
Référence	Règlement (UE) 2024/1689
Etat actuel	En vigueur
Date d'entrée en vigueur	01.08.2024
Unité responsable dans l'administration fédérale	OFCOM

Description

Le règlement établissant des règles harmonisées concernant l'intelligence artificielle (ci-après "règlement sur l'IA") est entré en vigueur le 1er août 2024. Il couvre en particulier le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle dans l'UE, qui doivent être conformes aux valeurs de l'UE. Le règlement établit ainsi une classification des systèmes d'IA, ainsi que différentes exigences et obligations adaptées selon une approche fondée sur les risques. Les nouvelles règles s'appliqueront principalement aux fournisseurs établis dans l'UE ou dans un pays tiers, et qui mettent des systèmes d'IA sur le marché européen ou qui les mettent en service dans l'UE, ainsi qu'aux déployeurs de systèmes d'IA situés dans l'UE. Le règlement sur l'IA s'applique également aux fournisseurs et aux déployeurs de systèmes d'IA situés dans un pays tiers, lorsque les résultats produits par le système d'IA sont utilisés dans l'UE.

Le règlement sur l'IA **interdit les systèmes ou applications d'IA** particulièrement préjudiciables et abusives, et qui entrent en contradiction avec les valeurs de l'UE, notamment les suivants:

- Systèmes d'IA utilisant des techniques subliminales;
- Systèmes d'IA qui exploitent les vulnérabilités d'un groupe spécifique d'individus;
- Notation sociale par les acteurs publics et privés (dans certains cas);
- Systèmes de catégorisation biométrique;
- Identification biométrique à distance, en temps réel, dans des espaces accessibles au public, à des fins répressives, avec quelques exceptions.

Le règlement sur l'IA prévoit que les **systèmes d'IA à haut risque** ne peuvent être mis sur le marché, mis en service ou utilisés que s'ils remplissent certaines exigences. La législation fait la distinction entre deux catégories de systèmes d'IA à haut risque:

a. Les systèmes d'IA sont destinés à être utilisés comme composant de sécurité d'un produit couvert par les actes législatifs d'harmonisation de l'UE énumérés à l'annexe I (ex. machines, jouets, aviation), ou le système d'IA constitue lui-même un tel produit;
b. Les systèmes d'IA à haut risque déployés dans huit domaines spécifiques, définis à l'annexe III du règlement;
    - Systèmes biométriques;
    - Gestion et exploitation des infrastructures critiques;
    - Enseignement ou formation professionnelle;
    - Emploi, gestion des travailleurs et accès à l'emploi indépendant;
    - Accès et jouissance de certains services et prestations privés et publics essentiels;
    - Systèmes d'IA utilisés par les forces de l'ordre;
    - Systèmes d'IA utilisés dans la gestion des migrations, de l'asile et des contrôles aux frontières;
    - Certains systèmes d'IA destinés à l'administration de la justice et aux processus démocratiques.

Les systèmes d'IA à haut risque doivent faire l'objet d'une évaluation de la conformité pour pouvoir accéder au marché.

En ce qui concerne les **modèles d'IA à usage général** (General purpose AI models, GPAI), le règlement prévoit des obligations applicables à tous les modèles d'IA à usage général et des obligations supplémentaires pour les

modèles GPAI qui comportent des risques systémiques. Tous les fournisseurs de GPAI – quel que soit le risque qu'ils présentent – sont soumis à des mesures de transparence, sur les données utilisées pour le pré-entraînement et l'entraînement des modèles, y compris les textes et les données protégés par le droit d'auteur. Les modèles présentant des risques systémiques sont soumis à des obligations supplémentaires, notamment l'obligation d'effectuer des tests contradictoires pour identifier et atténuer les risques systémiques, atténuer les risques systémiques qui peuvent résulter du développement, la mise sur le marché ou l'utilisation du modèle, et notifier les incidents.

Les fournisseurs de modèles GPAI peuvent s'appuyer sur des codes de bonne pratique pour démontrer qu'ils se conforment aux obligations du règlement, jusqu'à ce qu'une norme harmonisée soit publiée. Le Bureau de l'IA, établi au sein de la Commission européenne, facilitera la création de ces codes.

Les **systèmes d'IA qui ne présentent qu'un risque limité** doivent remplir des obligations de transparence. Les systèmes destinés à interagir avec des personnes physiques, par exemple, doivent être conçus et développés de sorte que les personnes physiques soient informées du fait qu'elles interagissent avec un système d'IA, comme un robot logiciel (chatbot).

La législation prévoit des **sanctions financières** importantes pour toute violation des obligations prévues par le règlement sur l'IA. Par exemple, les infractions concernant le non-respect des interdictions des pratiques d'IA sont passibles d'amendes administratives pouvant aller jusqu'à 35 millions d'euros ou jusqu'à 7% du chiffre d'affaires annuel mondial total pour l'exercice précédent. Le non-respect des dispositions relatives aux opérateurs ou aux organismes notifiés est passible d'amendes administratives pouvant aller jusqu'à 15 millions d'euros ou jusqu'à 3% du chiffre d'affaires annuel mondial total pour l'exercice précédent.

Avancement des travaux

Le règlement sur l'IA sera applicable deux ans après son entrée en vigueur, soit dès le 2 août 2026, à l'exception de certaines dispositions spécifiques:

- Les dispositions relatives aux pratiques interdites en matière d'IA seront applicables dès le 2 février 2025;
- Les dispositions relatives aux modèles d'IA à usage général seront applicables dès le 2 août 2025;
- Les dispositions relatives aux systèmes d'IA classés à haut risque liés aux produits couverts par la législation d'harmonisation de l'UE (Annexe I, section A) seront applicables dès le 2 août 2027.

Possibles conséquences pour la Suisse

Le règlement sur l'IA a des conséquences pour les opérateurs suisses. Concrètement, ceux qui souhaitent exporter vers l'UE des produits d'IA ou dotés de systèmes d'IA devront évaluer ou faire évaluer la conformité de leurs produits selon le règlement sur l'IA, si ceux-ci entrent dans la catégorie des systèmes d'IA à haut risque. Ces obligations créent de nouvelles entraves à l'exportation.

La Suisse dispose avec l'UE d'un accord sur la reconnaissance mutuelle en matière d'évaluation de la conformité (ARM) pour des produits issus de 20 secteurs. Le règlement sur l'IA aura des répercussions sur ces secteurs (en particulier les machines), car pour les produits contenant des composants d'IA, les obligations qu'il prévoit s'ajouteront aux exigences en matière d'accès au marché. Il est prévu d'examiner si l'accord ARM pourrait être étendu afin d'inclure les exigences en matière d'IA et réduire ainsi les éventuelles entraves au commerce. Préalablement, des dispositions équivalentes doivent être introduites dans le droit suisse. De plus, au vu des relations entre la Suisse et l'UE, on ignore toujours quand l'UE sera à nouveau prête à actualiser l'ARM.

Une analyse détaillée du règlement sur l'IA et de ses répercussions pour la Suisse est en cours. En effet, le 22 novembre 2023, le Conseil fédéral a demandé au DETEC (OFCOM) et au DFAE (Division Europe) un état des lieux sur les approches réglementaires possibles de l'IA. Le document doit être remis Conseil fédéral sous la forme d'un rapport public.

Mesures déjà prises en Suisse

Comme mentionné dans la réponse précédente, la Suisse dresse actuellement un état des lieux concernant les approches de réglementation en matière d'IA, et analyse entre autres les conséquences en Suisse des instruments internationaux, tels que le règlement sur l'IA. Le mandat pour la réalisation de ce document et de l'analyse du règlement sur l'IA a été octroyé à la Suisse, de sa propre initiative.

Mesure 2

Loi sur les services numériques (Digital Services Act)

Appellation complète de la mesure	Règlement relatif à un marché unique des services numériques
Type de mesure	Règlement
Référence	Règlement (UE) 2022/2065
Etat actuel	En vigueur
Date d'entrée en vigueur	16 novembre 2022
Unité responsable dans l'administration fédérale	OFCOM

Description

Le règlement sur les services numériques (Digital Services Act; DSA) est entré en vigueur le 16 novembre 2022 et a renouvelé le cadre réglementaire de l'UE sur les services intermédiaires en ligne. Il prévoit des règles uniformes régissant les droits et responsabilités des services numériques, notamment des plateformes, dans le traitement des contenus illégaux et/ou préjudiciables en ligne. Les obligations inscrites dans le DSA sont cumulables: les services présentant le profil de risque le plus élevé (notamment les très grandes plateformes en ligne) doivent remplir toutes les obligations, tandis que les fournisseurs moins importants ou ayant une orientation différente ne doivent en remplir qu'une partie. Les différents services sont soumis, entre autres, aux obligations suivantes:

Obligations applicables à tous les services intermédiaires

- Tous les services intermédiaires doivent désigner un représentant qui fait office de point de contact unique.
- S'ils ne disposent pas d'un établissement dans l'UE, ils doivent désigner un représentant légal à l'intérieur de l'UE. Celui-ci peut être tenu explicitement responsable du non-respect des obligations prévues dans le DSA.
- Ils doivent publier chaque année un rapport de transparence décrivant leurs pratiques en matière de modération des contenus.
- Ils sont tenus d'informer les autorités judiciaires ou administratives nationales de la suite donnée à des injonctions de supprimer un contenu ou de fournir des informations.

Obligations de diligence applicables aux hébergeurs, plateformes en ligne comprises

- Tous les hébergeurs doivent disposer d'un système permettant aux utilisateurs et aux organisations de signaler les contenus qu'ils considèrent comme illégaux.
- Ils doivent justifier clairement auprès des utilisateurs concernés les restrictions qu'ils apportent aux services qu'ils leur fournissent, et ce au plus tard au moment où ils mettent en place les restrictions.
- S'ils soupçonnent une activité criminelle menaçant la vie ou la sécurité d'une personne, ils doivent la signaler aux autorités compétentes.

Obligations de diligence supplémentaires applicables aux plateformes en ligne

- Les plateformes en ligne doivent disposer d'un système de plainte interne permettant aux utilisateurs de contester les mesures de restriction qu'elles décident.
- Les plateformes qui diffusent de la publicité doivent s'assurer que les utilisateurs peuvent l'identifier comme telle. L'annonceur et la source de financement de la publicité (si celle-ci est différente), ainsi que les paramètres utilisés pour la diffusion de la publicité doivent être clairement indiqués. La publicité basée sur le profilage de données sensibles est interdite.

Dispositions applicables aux fournisseurs de plateformes en ligne conçues pour permettre aux consommateurs de conclure des contrats à distance avec des professionnels

- Les fournisseurs concernés veillent à ce que les entreprises ne puissent utiliser leur plateforme que si elles ont reçu certaines informations nécessaires.
- Les fournisseurs concernés vérifient que les entreprises qui utilisent leur plateforme sont en mesure de respecter la législation en vigueur en matière d'informations précontractuelles, de conformité et de sécurité des produits. Ils doivent également s'assurer que les informations de contact nécessaires sont disponibles.

Obligations de diligence supplémentaires pour les très grandes plateformes en ligne (en moyenne plus de 45 millions d'utilisateurs actifs dans l'UE)

- Les très grandes plateformes en ligne doivent procéder chaque année à une évaluation des risques et prendre des mesures concrètes pour les réduire. Cette évaluation inclut les risques systémiques, y compris la diffusion de contenus illégaux, ainsi que les risques liés aux droits fondamentaux et à la communication publique.
- Dans les cas de crise, elles peuvent se voir obligées de prendre des mesures spécifiques, sur décision de la Commission européenne (COM).
- Elles doivent se soumettre chaque année à un audit indépendant sur leurs processus et sur leurs obligations.
- Elles doivent proposer au moins un système de recommandation qui ne repose pas sur le profilage.
- S'agissant de la publicité en ligne, elles doivent mettre en place un registre de données accessible au public (qui inclue notamment le contenu des publicités diffusés, les annonceurs et le financement, le modèle de profilage, le nombre de personnes atteintes).
- Elles doivent permettre aux autorités de surveillance compétentes d'accéder, sur demande, aux données nécessaires à l'application du DSA. Ces autorités peuvent en outre exiger que des chercheurs agréés aient accès aux données.
- Elles doivent présenter un rapport de transparence tous les 6 mois et fournir des éléments supplémentaires (notamment les ressources en personnel consacrées à la modération des contenus et les mesures de réduction des risques mises en place).

La **surveillance et l'application** du DSA incombent aux Etats membres de l'UE et à leurs autorités nationales de surveillance pour les services intermédiaires, les hébergeurs et les plateformes en ligne. La surveillance des très grandes plateformes relève exclusivement de la compétence de la COM. En cas de non-respect des obligations, les amendes s'élèvent au maximum à 6% du chiffre d'affaires global annuel, et jusqu'à 1% si les informations fournies sont erronées, incomplètes ou trompeuses.

Jusqu'en octobre 2024, la COM avait qualifié 25 services de très grandes plateformes en ligne et très grands moteurs de recherche en ligne. Il s'agit entre autres d'AliExpress, Amazon, Apple Store, Booking, Google Search, Google Maps, LinkedIn, Facebook, Instagram, Microsoft Bing, Pinterest, Pornhub, Snapchat, Tik Tok, X, Youtube et Zalando.

Situation actuelle

Entré en vigueur le 16 novembre 2022, le règlement est pleinement applicable depuis le 17 février 2024. Dans le cadre de la mise en œuvre de la législation, la Commission a lancé des procédures formelles d'infraction contre TikTok, AliExpress, Facebook, Instagram et X. En avril 2024, elle a entamé des procédures d'infraction contre six Etats membres (Tchéquie, Estonie, Pologne, Portugal, Slovaquie, Chypre), lesquels n'ont pas encore désigné leur coordinateur national pour les services numériques (délai 17 février 2024).

Possibles conséquences pour la Suisse

Actuellement, la Suisse ne dispose d'aucune législation spécifique aux services intermédiaires en ligne. Toutefois, le DSA aura des répercussions directes et indirectes sur la Suisse et sur les fournisseurs de services intermédiaires en ligne domiciliés en Suisse.

Le règlement ne s'applique pas seulement aux fournisseurs situés sur le territoire de l'UE, mais à tous ceux, quel que soit leur lieu d'établissement, qui offrent des services à des clients qui se trouvent dans un Etat membre de l'UE. En d'autres termes, les fournisseurs suisses de services en ligne actifs sur le marché intérieur de l'UE y sont eux aussi soumis. Or, à l'heure actuelle, aucune entreprise suisse ne peut être qualifiée de très grande plateforme

en ligne selon les critères fixés dans le DSA. Par conséquent, les obligations les plus strictes ne s'appliqueront pas directement aux fournisseurs suisses.

Toutefois, pour faciliter l'application des règles, l'UE mise sur une obligation de désigner un représentant juridique ayant son siège social dans le marché intérieur de l'UE. Cette obligation concerne donc tous les services intermédiaires suisses qui proposent leurs services dans l'UE. Le représentant peut être tenu directement responsable en cas d'infraction au règlement (et notamment se voir infliger des amendes). Etant donné que, pour les entreprises suisses, cette obligation constitue *de facto* un obstacle non négligeable à l'accès au marché, dans les cas ordinaires, il convient de maintenir les coûts liés à cette représentation dans certaines limites. Dans la pratique, il peut s'agir de faire couvrir plusieurs réglementations de l'UE par un même représentant.

En ce qui concerne les effets indirects, il est possible que les plateformes étrangères appliquent certaines normes de l'UE à la Suisse, celle-ci étant souvent considérée comme faisant partie du même marché pour les services offerts au niveau international. Toutefois, les plateformes sont tout à fait en mesure d'exploiter des solutions spécifiques à chaque pays, ce qu'elles font si elles y trouvent leur compte. En tout état de cause, les utilisateurs suisses ne peuvent pas faire valoir en Suisse les mécanismes de protection prévus par le DSA et applicables aux citoyens de l'UE. Ces mécanismes n'interviendraient en Suisse que sur la base d'un engagement volontaire des intermédiaires. Les utilisateurs suisses sont donc tendanciellement moins bien lotis que ceux de l'UE, même si les intermédiaires effectuaient certaines adaptations techniques exigées par le DSA pour la Suisse également.

Mesures déjà prises en Suisse

Le 5 avril 2023, le Conseil fédéral a chargé le DETEC (OFCOM) d'élaborer un projet de consultation sur la réglementation des grandes plateformes de communication. Le projet poursuit un objectif plus étroit que celui du DSA et se concentre sur des aspects pertinents pour la communication publique et la formation de l'opinion. Dans ces domaines, il convient de renforcer les droits des utilisateurs, et les plateformes doivent améliorer la transparence. Le projet de consultation s'inspirera, au besoin, des règles du DSA, mais la décision d'agir sur le plan réglementaire a été prise indépendamment de ce règlement. Le projet est prévu pour début 2025.

Aucune mesure n'est actuellement prévue en Suisse dans d'autres domaines du DSA, comme la protection contre les produits illégaux, contrefaits ou dangereux.

Mesure 3

Loi sur les marchés numériques (Digital Services Act)

Appellation complète de la mesure	Règlement relatif aux marchés contestables et équitables dans le secteur numérique
Type de mesure	Règlement
Référence	Règlement (UE) 2022/1925
Etat actuel	En vigueur
Date d'entrée en vigueur	1er novembre 2022
Unité responsable dans l'administration fédérale	SECO

Description

Le 1er novembre 2022, le règlement sur les marchés numériques (Digital Markets Act; DMA) est entré en vigueur. Il établit une série de nouvelles règles ex ante pour certaines grandes plateformes en ligne, appelées contrôleurs d'accès (*gatekeepers*), dans le but de garantir la contestabilité et l'équité sur les marchés numériques. le DMA complète le droit de la concurrence.

Une entreprise est désignée comme un contrôleur d'accès si elle remplit les critères suivants :

- elle exploite (dans au moins trois Etats membres de l'UE) au moins un service de plateforme centrale, tel qu'un moteur de recherche, un réseau social, une plateforme de partage de vidéos, un service de messagerie, un système d'exploitation, un navigateur web, un service de cloud computing, des services de publicité en ligne ou des services intermédiaires en ligne (p. ex. App-Store);
- elle a réalisé un chiffre d'affaires annuel dans l'Union supérieur ou égal à 7,5 milliards d'euros au cours de chacun des trois derniers exercices, ou sa capitalisation boursière moyenne a atteint au moins 75 milliards d'euros au cours du dernier exercice;
- elle fournit un service de plateforme essentiel, qui compte au moins 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et au moins 10 000 entreprises utilisatrices actives par an établies dans l'Union.

Les contrôleurs d'accès doivent entre autres :

- veiller à ce que le désabonnement des services de plateformes essentiels soit aussi facile que l'abonnement;
- veiller à ce que les fonctionnalités de base des services de messagerie instantanée soient interopérables;
- donner aux entreprises utilisatrices l'accès à leurs données de performance marketing ou publicitaire sur la plateforme;
- n'utiliser les données qu'en fonction du produit;
- informer la Commission européenne (COM) des acquisitions et fusions qu'elles réalisent.

Les contrôleurs d'accès ne pourront plus entre autres :

- classer leurs propres produits ou services de manière plus favorable que ceux des autres acteurs du marché (auto-préférence);
- préinstaller certaines applications ou certains logiciels, ou empêcher les utilisateurs de désinstaller facilement ces applications ou logiciels;
- imposer que les logiciels les plus importants (p. ex. navigateurs web) soient installés par défaut à l'installation du système d'exploitation;
- réutiliser les données personnelles collectées lors d'une prestation pour les besoins d'une autre prestation.

Si un contrôleur d'accès enfreint les règles fixées par le règlement DMA, il risque une amende allant jusqu'à 10%, et, en cas de récidive, jusqu'à 20% de son chiffre d'affaires mondial.

La COM est responsable de la désignation des entreprises comme contrôleurs d'accès. Lorsqu'une entreprise atteint les seuils pertinents pour être désignée, elle doit le lui notifier au plus tard dans les deux mois qui s'ensuivent. Si une entreprise ne fournit pas les informations pertinentes, la COM est habilitée à la désigner unilatéralement sur la base des informations dont elle dispose. Elle est la seule instance habilitée à faire appliquer les règles et les obligations prévues dans le règlement DMA. Afin de soutenir la COM, les Etats membres ont la possibilité d'autoriser leurs autorités nationales chargées de l'application des règles de concurrence à mener des enquêtes sur le non-respect éventuel du règlement et à lui rapporter les résultats.

Situation actuelle

La législation est entrée en vigueur le 1er novembre 2022 et est pleinement applicable depuis le 7 mars 2024. Jusqu'en octobre 2024, la COM avait désigné un total de **7 contrôleurs d'accès** — **Alphabet, Amazon, Apple, Booking, ByteDance, Meta et Microsoft**. Au total, 24 services fournis par des contrôleurs d'accès ont été désignés.

Le 25 mars 2024, la COM a ouvert une procédure à l'encontre d'Alphabet, d'Apple et de Meta, qu'elle soupçonne de diverses violations du DMA. Elle entend vérifier si l'affichage des résultats de recherche Google par Alphabet conduit à privilégier ses propres services de recherche en aval (p. ex. pour les marchandises, les vols ou les hôtels) par rapport aux fonctions de recherche similaires des fournisseurs concurrents.

Possibles conséquences pour la Suisse

Le règlement DMA s'applique à toutes les entreprises actives dans l'UE. Toutefois, aucune entreprise ayant son siège en Suisse ne pourrait encore être considérée comme contrôleur d'accès au sens du DMA. C'est pourquoi il ne s'applique actuellement qu'aux entreprises dont le siège se situe en Suisse et qui utilisent, à titre commercial dans l'UE, un service de plateforme centrale fourni par un contrôleur d'accès.

La question se pose de savoir dans quelle mesure le DMA aura des effets indirects en Suisse, car les contrôleurs d'accès y appliqueront d'eux-mêmes les nouvelles règles. Pour l'heure, diverses pratiques coexistent. Selon une annonce faite par Meta, l'entreprise applique le DMA en Suisse (sur ses services de plateforme Facebook, Instagram, Whatsapp, Messenger, Marketplace, Ads). Microsoft dit aussi le faire sur son service de plateforme central Linkedin, mais pas encore complètement sur son service de plateforme central Windows. Apple (App Store, Safari, iOS), Bytedance (TikTok) et Alphabet (Google Search, Google Ads, Chrome, Google Maps, Google Play, Google Shopping, Youtube, Google Android) n'appliquent pas entièrement le DMA (du moins pas encore). Quant à Amazon (Marketplace, Ads), les utilisateurs semblent être soumis aux règles du marché suisse. Enfin, Booking n'a encore rien annoncé.

Mesures déjà prises en Suisse

Le DMA s'inspire essentiellement du droit européen de la concurrence, de sorte que plusieurs de ses réglementations ex ante pourraient aussi être appliquées par le biais du droit de la concurrence. De la même manière, en Suisse, les dispositions du DMA doivent correspondre au contrôle des abus prévu dans le droit des cartels (art. 7 LCart) (voir également la motion 23.3069 Créer une loi sur les marchés numériques pour la Suisse). Dans certains cas, les autorités de la concurrence peuvent en outre ordonner des mesures provisionnelles, par exemple pour contrer la menace de fermetures irréversibles de marchés.

Depuis le 1er décembre 2022, les clauses de parité concernant le prix, la disponibilité ou d'autres conditions fixées dans les contrats entre les plateformes de réservation en ligne et les établissements d'hébergement sont interdites en Suisse (art. *8a* LCD). Une disposition comparable existe également dans le DMA (art. 5, al. 3), mais elle ne se limite toutefois pas au domaine de l'hébergement. Par contre, elle ne s'applique qu'aux très grandes plateformes, alors que la réglementation de la LCD s'applique à toutes les plateformes en ligne. La réglementation inscrite dans la LCD ne l'a pas été en réaction au DMA; il s'agit d'une réponse à la motion 16.3902 Bischof.

Mesure 4

Règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants

Appellation complète de la mesure	Proposition de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants
Type de mesure	Proposition de règlement
Référence	Proposition de règlement COM/2022/209 final
Etat actuel	Processus législatif en cours
Date d'entrée en vigueur	Pas encore adoptée
Unité responsable dans l'administration fédérale	fedpol

Description

Le 11 mai 2022, la Commission européenne (COM) a publié une proposition de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants (proposition concernant les abus sexuels sur enfants; Child Sexual Abuse Proposal - CSA). Parallèlement à cette proposition, elle a présenté une nouvelle Stratégie européenne pour un internet meilleur pour les enfants.

L'UE a fait de la protection des enfants (en ligne et hors ligne) une de ses priorités. Par le passé, la COM a demandé aux entreprises d'intensifier leurs efforts pour détecter, signaler et supprimer les contenus illégaux en ligne. Ces mesures volontaires se sont révélées insuffisantes, et plusieurs Etats membres ont édicté des dispositions nationales afin de combattre les abus sexuels impliquant des enfants sur internet. Celles-ci ont conduit à une fragmentation croissante du marché intérieur des services numériques. La proposition de la COM vise à établir un cadre juridique clair et harmonisé.

La proposition de règlement se compose de deux éléments principaux:

1. Obligations imposées aux fournisseurs en matière de détection, de signalement, de suppression et de blocage de matériel pédopornographique:
    - Les fournisseurs, quel que soit leur lieu d'établissement, doivent détecter dans leurs services, signaler et supprimer tout matériel lié à des abus sexuels sur des enfants. Les signalements sont transmis au nouveau centre européen, qui reste à créer.
    - Les magasins d'applications (app stores) doivent veiller à ce que les enfants ne puissent pas télécharger des applications présentant un risque élevé d'être utilisées par des agresseurs potentiels qui chercheraient à entrer en contact avec eux.
    - Les hébergeurs ou les fournisseurs de services de messagerie doivent évaluer les risques de détournement de leurs services à des fins de diffusion de matériel pédopornographique ou de sollicitation d'enfants ("grooming").
    - Les Etats membres doivent désigner des autorités nationales chargées d'examiner l'évaluation des risques.
2. Création d'un organe central de l'UE en tant qu'agence décentralisée qui permette la mise en œuvre du nouveau règlement.

Les fournisseurs de services s'engagent, dans leurs mesures, à protéger la sphère privée de leurs utilisateurs. Les vérifications nécessaires sont effectuées de manière anonyme. Les mesures d'identification des utilisateurs peuvent être prises exclusivement en cas de soupçon d'abus sexuel sur des enfants. La technologie utilisée doit extraire uniquement les informations strictement nécessaires à la détection de l'abus. **La proposition actuelle de la COM ne prévoit pas de surveillance étatique continue et sans motif de toutes les communications numériques interpersonnelles.** Néanmoins, la publication de la proposition a provoqué de vives réactions, notamment contre l'injonction de détection et contre le cryptage de bout en bout.

Situation actuelle

Actuellement, la proposition de règlement CSA est discutée au Conseil de l'UE et, parallèlement, au Parlement de l'UE. L'injonction de détection ainsi que la détection, au moment du cryptage, du matériel crypté de bout en bout sont particulièrement controversées. Le projet a été remanié plusieurs fois et d'autres propositions ont été faites. Toutefois, aucun accord n'a pu être trouvé à ce jour. La présidence hongroise du Conseil a repris le dossier et a présenté une nouvelle proposition de compromis qui n'a finalement pas été soumise au vote. Actuellement, il existe toujours une minorité de blocage (DE, AT, LUX, IT, NL, PL, SK, EE), dont un seul État membre devrait être d'accord ou s'abstenir pour qu'une proposition de compromis soit adoptée.

On ignore donc encore si et quand la proposition de règlement CSA sera mise en œuvre et si elle comprendra l'injonction de détection.

Possibles conséquences pour la Suisse

Le règlement CSA ne représente pas un développement de l'acquis de Schengen. Néanmoins, les personnes ayant leur siège ou leur domicile en Suisse pourraient éventuellement être concernées par les règles proposées et, par conséquent, par l'injonction de détection.

Ces injonctions de détection entreraient probablement en conflit avec le droit suisse. En effet, selon l'art. 271 CP, est punissable quiconque accomplit pour un Etat étranger, sur le territoire suisse et sans autorisation, des actes qui relèvent d'une autorité ou d'un fonctionnaire, accomplit de tels actes pour une autorité étrangère ou une autre organisation de l'étranger, ou quiconque facilite de tels actes. Est également soumis au droit suisse quiconque commet un tel délit à l'étranger (art. 4, al. 1, CP).

Mesures déjà prises en Suisse

En 2022, au Conseil national, la proposition de règlement CSA a donné lieu à l'Interpellation 22.3404 Bellaiche du 9 mai 2022, "Contrôle des messageries instantanées" et à la Motion 22.4113 Bellaiche du 29 septembre 2022, "Contrôle des messageries instantanées. Protéger la population contre une surveillance généralisée continue et sans motif". Le Conseil fédéral a été chargé de faire respecter le droit à la protection de la sphère privée garanti par l'art. 8 CEDH et l'art. 13 Cst., et de protéger les habitants de la Suisse contre le contrôle des messageries instantanées prévu dans la proposition de règlement CSA.

Dans son avis du 23 novembre 2022, le Conseil fédéral a indiqué qu'il n'était pour l'heure pas possible d'évaluer de manière définitive les conséquences pour la Suisse. Il a annoncé examiner la nécessité d'agir en matière de protection des enfants et des jeunes sur internet ainsi que des effets de la proposition de règlement CSA, afin de pouvoir identifier à temps les éventuelles mesures à prendre.

Le 27 avril 2023, après avoir entendu le PFPDT, la Commission des affaires juridiques du Conseil national (CAJ-N) a communiqué qu'elle accorderait une attention particulière à la manière dont le contrôle des messages de chat évoluerait dans l'UE et aux conséquences que cela pourrait avoir pour la population suisse. Le 25 septembre 2023, le Conseil national a clairement adopté la motion.

Le rapport du DFJP annoncé par le Conseil fédéral a été publié le 27 septembre 2024.

Mesure 5

Règlement sur l’identité numérique européenne

Appellation complète de la mesure	Règlement modifiant le règlement (UE) n° 910/2014 en ce qui concerne l’établissement du cadre européen relatif à une identité numérique
Type de mesure	Règlement
Référence	Règlement (UE) 2024/1183
Etat actuel	Entré en vigueur
Date d’entrée en vigueur	20.05.2024
Unité responsable dans l’administration fédérale	OFJ

Description

Le règlement sur l’identité numérique européenne (eID) est entré en vigueur le 20 mai 2024. Il modifie le règlement (UE) 910/2014 eIDAS de 2014 et crée le cadre nécessaire pour une identité numérique européenne. Il remédie aux lacunes du système eIDAS en améliorant l’efficacité du cadre et en étendant ses avantages au secteur privé. Les Etats membres offriront aux citoyens et aux entreprises des portefeuilles numériques (e-wallets), qui relieront différents aspects de leur identité numérique nationale. Ces portefeuilles seront fournis par des autorités publiques ou par le secteur privé, à condition d’être reconnus par les Etats membres. Les consommateurs pourront également accéder à des services en ligne sans devoir recourir à des plateformes privées ni partager inutilement des données personnelles.

Les principaux éléments de l'acte révisé peuvent être résumés comme suit :

- D'ici 2026, chaque Etat membre doit mettre un portefeuille d'identité numérique à la disposition de ses citoyens et accepter les portefeuilles européens d'identité numérique provenant d'autres Etats membres conformément au règlement révisé.
- Des garanties suffisantes permettent d’éviter toute discrimination à l'encontre des personnes qui choisissent de ne pas avoir recours au portefeuille, dont l'utilisation se fera toujours sur une base volontaire.
- Selon le modèle économique du portefeuille, la délivrance, l'utilisation et la révocation sont gratuites pour toutes les personnes physiques.
- S’agissant de la validation des attestations électroniques d'attributs, les Etats membres sont tenus de fournir gratuitement des mécanismes de validation ayant pour unique but de vérifier l'authenticité et la validité du portefeuille et l'identité des parties utilisatrices.
- S’agissant du code pour les portefeuilles, les composants logiciels pour les applications reposent sur un code source ouvert, mais les Etats membres disposent d'une marge de manœuvre afin que, pour des raisons justifiées, des composants spécifiques autres que ceux installés sur les appareils utilisateurs ne soient pas soumis à l’obligation de divulgation.
- La cohérence entre le portefeuille en tant que forme d'identification électronique et le système dans le cadre duquel il est délivré a été assurée.

Enfin, le règlement révisé clarifie le champ d'application des certificats qualifiés d'authentification de site internet, garantissant ainsi que les utilisateurs peuvent vérifier qui sont les administrateurs d'un site internet, tout en préservant les règles et normes de sécurité actuelles bien établies du secteur.

Situation actuelle

Le règlement eID modifiant le règlement eIDAS est entré en vigueur le 20 mai 2024 et doit être pleinement mis en œuvre d'ici 2026.

Possibles conséquences pour la Suisse

La Suisse n'a pas d'obligation juridique d'adopter le règlement eIDAS et les modifications qui s'y rapportent. Toutefois, compte tenu de l'étroitesse des rapports commerciaux et sociaux qu'elle entretient avec la plupart des pays membres de l'UE, elle a tout intérêt à rendre son système d'identité électronique interopérable avec celui de l'Union.

Afin d'être reconnue par les Etats membres, l'e-ID suisse devra être acceptée dans le cadre du processus de notification, qui nécessite un traité international. La reprise unilatérale du règlement eIDAS en droit suisse semble peu avantageuse, le but étant d'assurer la reconnaissance réciproque des systèmes suisse et européen (et non uniquement la reconnaissance du système suisse dans l'UE).

Le projet de loi sur l'e-ID prévoit que le Conseil fédéral peut conclure des accords internationaux afin d'obtenir une reconnaissance internationale de l'e-ID et de reconnaître les e-ID étrangères (art. 31). Il permet ainsi d'obtenir une reconnaissance mutuelle, notamment avec l'UE.

La mise en place de l'e-ID et de l'infrastructure de confiance ne fait pas l'objet des négociations avec l'Union européenne concernant les accords bilatéraux du nouveau paquet.

Mesures déjà prises en Suisse

Après le rejet par le peuple de la loi fédérale sur les services d'identification électronique, le 7 mars 2021, le Conseil fédéral a chargé le Département fédéral de justice et police d'esquisser une solution d'identification électronique étatique, en collaboration avec la Chancellerie fédérale et le Département fédéral des finances. Entre temps, le Conseil national et le Conseil des Etats ont approuvé six motions identiques, émanant de tous les groupes parlementaires et demandant la mise en place d'un système géré par l'Etat qui permette de prouver son identité en ligne.

Le 22 novembre 2023, le Conseil fédéral a adopté le message et le nouveau projet de loi sur l'e-ID. Les délibérations parlementaires ont débuté en janvier 2024. La Commission des affaires juridiques du Conseil National (CAJ-N) a adopté le texte par 21 voix contre 0 et 3 abstentions, et le Conseil national (plénum) par 175 voix contre 12 et 2 abstentions. Les délibérations au deuxième conseil ont débuté en mars 2024 et se sont poursuivies jusqu'à la session d'automne 2024. Etant donné que des divergences subsistent entre les conseils, celles-ci font actuellement l'objet d'une procédure d'élimination des divergences.

Le nouveau projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID) prévoit la mise en place d'une identité électronique étatique gratuite et volontaire pour les titulaires d'un document d'identité émis par les autorités suisses. Dans ce cadre, l'Etat continue d'assumer sa tâche centrale qu'est la vérification de l'identité d'une personne ainsi que l'émission de la preuve électronique s'y rapportant. Comme le demandent les motions déposées au Conseil national, le nouveau projet poursuit une approche fondée sur les principes du respect de la vie privée dès la conception et par défaut, de l'économie des données et de l'enregistrement décentralisé des données.

En outre, le projet de loi vise à créer une infrastructure de confiance étatique permettant aux acteurs des secteurs public et privé d'émettre et d'utiliser des preuves électroniques. Dans ce cadre, l'Etat exploitera les systèmes de base nécessaires (registre de base, registre de confiance) et offrira un portefeuille électronique étatique sous forme d'application mobile, qui pourra contenir l'e-ID et d'autres moyens de preuves électroniques. Les titulaires du portefeuille électronique pourront présenter leur e-ID et autres moyens de preuves électroniques de manière sécurisée et transparente.

Mesure 6

Règlement sur la gouvernance des données (Data Governance Act)

Appellation complète de la mesure	Règlement portant sur la gouvernance européenne des données
Type de mesure	Règlement
Référence	Règlement (UE) 2022/868
Etat actuel	En vigueur
Date d'entrée en vigueur	23.06.2022
Unité responsable dans l'administration fédérale	OFCOM/OFJ

Description

Le Règlement (UE) 2022/868 sur la gouvernance européenne des données, entré en vigueur le 23 juin 2022, est destiné à encourager la circulation des données dans le marché unique. Il vise à stimuler la réutilisation des données sensibles détenues par des organismes du secteur public et protégées pour des raisons de confidentialité commerciale, de secret statistique, de protection des droits de propriété intellectuelle de tiers ou de protection des données à caractère personnel (comme les données dans les domaines de l'énergie, du transport et les données médicales). Jusqu'ici la Directive PSI 2019/1024 a permis de faciliter la réutilisation des données du secteur public, mais elle exclut explicitement de son champ d'application les données dites sensibles.

Le règlement s'articule autour de trois priorités:

1. Etablir **des conditions spécifiques qui encouragent et autorisent la réutilisation** des certaines données du secteur public protégées par le droit de la propriété intellectuelle, la confidentialité des données statistiques, la protection des données ou le secret commercial;
2. Introduire des principes communs pour les intermédiaires de données, tel qu'un **cadre d'inscription et de supervision pour les services de partage de données**;
3. Encourager l'altruisme des données en introduisant un cadre pour **l'enregistrement volontaire** des entités qui collectent et traitent ce genre des données.

Les données détenues par des entreprises publiques (telles que les radiodiffuseurs de service public, les établissements culturels ou d'enseignement et les données touchant à la sécurité publique) sont exclues du champ d'application (art. 3).

Le règlement ne prévoit pas d'obligation de traiter ou de stocker des données dans l'UE, ni d'obligation d'établissement dans l'UE pour les Etats tiers. La Commission européenne prévoit d'adopter des actes d'exécution attestant que les dispositifs mis en œuvre dans des Etats tiers pour protéger la propriété intellectuelle et les secrets d'affaires assurent une protection essentiellement équivalente à celle de l'UE.

Situation actuelle

Le règlement est entré en vigueur le 23 juin 2022. Les nouvelles règles sont applicables depuis le mois de septembre 2023. En août 2023, la Commission a mis en place, au moyen d'un règlement d'exécution, des logos communs permettant d'identifier facilement les prestataires de services d'intermédiation de données de confiance et les organisations altruistes en matière de données dans l'UE.

En mai 2024, la Commission a ouvert des procédures d'infraction en envoyant une lettre de mise en demeure à 18 Etats membres qui n'avaient pas désigné les autorités responsables de la mise en œuvre de l'acte sur la gouvernance des données ou qui n'avaient pas prouvé que ces dernières étaient habilitées à exécuter les tâches requises par le règlement.

Possibles conséquences pour la Suisse

Le règlement n'est pas contraignant pour la Suisse. Les directives relatives à la transmission de données confidentielles détenues par des organismes publics ainsi que les exigences légales applicables aux intermédiaires de données ne valent donc pas pour la Suisse.

Le règlement ne libère pas les organes de l'UE concernés de leurs obligations de confidentialité et les accords internationaux restent réservés (voir art. 3, al. 3, du règlement). Par conséquent, les données obtenues par un organe de l'UE au moyen de l'assistance administrative de l'étranger (p. ex. de la Suisse) ne devraient pas être concernées par l'application, puisque que les accords d'assistance administrative contiennent des réserves de spécialité et de confidentialité.

Certaines entreprises suisses sont toutefois concernées, comme les intermédiaires de données qui proposent leurs services dans l'UE sans y être établis (p. ex. établis en Suisse), et devront respecter certaines règles, notamment désigner un représentant légal dans un Etat membre (voir art. 11, al. 3).

Le règlement s'applique aussi au transfert de données confidentielles non personnelles depuis des organismes publics de l'UE vers la Suisse. Par conséquent, les réutilisateurs de ces données ne sont habilités à organiser des transferts vers des pays tiers (p. ex. la Suisse) que si des mesures de protection adéquates existent dans ces pays pour ce type de données. Les garanties requises sont réputées exister si le niveau de protection des secrets commerciaux et de la propriété intellectuelle correspond en substance à celui de l'UE. La COM peut adopter des actes d'exécution établissant qu'un pays tiers offre un niveau de protection adéquat. Cette procédure se distingue de la procédure de décision d'adéquation inscrite dans le RGPD et applicable au transfert de toutes les données à caractère personnel vers des pays tiers. La Suisse peut vraisemblablement faire valoir ces mesures puisqu'elle protège les secrets commerciaux et la propriété intellectuelle de manière similaire à l'UE. Concrètement, ce cas ne devrait concerner que très peu d'entreprises ou d'organismes (p. ex. des instituts de recherche ou des universités), à savoir celles qui souhaitent accéder à des données confidentielles publiées par des organismes publics de l'UE et les transférer en Suisse.

La Suisse est en outre indirectement concernée en tant que membre du Système statistique européen (SSE) (accord sur les statistiques passé dans le cadre des négociations bilatérales II). Le règlement a une influence directe sur la production statistique des Etats membres de l'UE. Tôt ou tard, cela apparaîtra également dans les réglementations de la production statistique européenne et sera éventuellement intégré dans l'accord statistique bilatéral UE-CH.

Mesures déjà prises en Suisse

Pour répondre à la motion 22.3890 Elaboration d'une loi-cadre sur la réutilisation des données du Conseil des Etats, le Conseil fédéral a été chargé de créer les bases nécessaires afin que des infrastructures spécifiques permettant de réutiliser des données dans les domaines stratégiques soient rapidement développées et mises en place. L'OFJ a pris connaissance du règlement sur la gouvernance des données dans le cadre de ses travaux législatifs habituels. Pour le moment, il n'a pas encore été décidé si et dans quelle mesure celui-ci sera intégré au projet de loi.

Mesure 7

Règlement sur les données (Data Act)

Appellation complète de la mesure	Règlement concernant des règles harmonisées portant sur l'équité de l'accès aux données
Type de mesure	Règlement
Référence	Règlement (UE) 2023/2854
Etat actuel	En vigueur
Date d'entrée en vigueur	11.01.2024
Unité responsable dans l'administration fédérale	OFCOM/OFJ

Description

Le règlement (UE) 2023/2854 sur les données (Data Act), entré en vigueur en janvier 2024, précise qui peut utiliser les données personnelles et non-personnelles générées dans l'UE, qui peut accéder à ces données et à quelles conditions.

Le règlement vise à fournir une législation horizontale pour le partage des données industrielles en introduisant l'obligation de donner aux utilisateurs l'accès aux données qu'ils contribuent à générer et de garantir aux organismes publics l'accès aux données détenues par des particuliers dans des circonstances exceptionnelles. Les fabricants de produits connectés et les fournisseurs de services connexes, appelées data holders, devront donc fournir aux utilisateurs un accès facile, immédiat et gratuit aux données que ceux-ci ont contribué à générer. Les utilisateurs pourraient décider de partager ces données avec des tiers, lesquels ne pourraient toutefois pas les utiliser pour développer des produits concurrents. Des mesures spécifiques sont incluses pour éviter que des tiers n'extorquent ou ne manipulent le consentement au partage des données. En outre, les grandes plateformes en ligne désignées comme gatekeepers en vertu de la législation sur les marchés numériques (DMA) ne constituent pas des tiers admissibles.

Le règlement précise les conditions dans lesquelles les détenteurs de données les mettent à la disposition des destinataires de données et spécifie que cela doit se faire dans des conditions équitables, raisonnables, non-discriminatoires et de manière transparente. Un test d'équité est inclus pour empêcher l'imposition de conditions contractuelles abusives aux petites et moyennes entreprises.

Le règlement donne aux institutions publiques le pouvoir de demander l'accès à des données considérées comme essentielles pour répondre à des urgences publiques, telles que des attaques terroristes et des catastrophes naturelles. Les demandes doivent être proportionnées et se limiter à la crise à laquelle elles sont censées répondre. Les micros ou petites entreprises sont exemptées des obligations de partage de données.

Le règlement introduit également des règles sur l'interopérabilité et la possibilité de changer de fournisseur de services de traitement de données en nuage (cloud switching). Il prévoit que les contrats doivent permettre le passage à un autre service dans un délai de 30 jours, et garantir une assistance complète ainsi que la continuité du service pendant la transition. Après trois ans, le "service de sortie" devra être fourni gratuitement. Les services en nuage devront garantir la compatibilité avec les interfaces ouvertes ou les normes d'interopérabilité établies au niveau européen.

Le règlement adopte un régime similaire à celui des données personnelles en obligeant les services en nuage à assurer des garanties appropriées pour empêcher les transferts internationaux de données industrielles ou un accès, par un gouvernement tiers, incompatible avec la législation européenne ou nationale.

Situation actuelle

Le règlement, entré en vigueur le 11 janvier 2024 et s'appliquera à partir du 12 septembre 2025.

Possibles conséquences pour la Suisse

Le règlement sur les données ne s'applique pas directement à la Suisse. Il vaut toutefois non seulement pour les détenteurs de données, les destinataires de données et les fournisseurs de produits et de services établis sur le territoire de l'UE, mais aussi pour tous les fournisseurs, quel que soit leur lieu d'établissement, qui proposent des produits et des services pertinents ou des données à des clients situés dans les Etats membres de l'UE, ou qui y reçoivent des données.

Certaines entreprises suisses sont donc également concernées, notamment celles qui:

- proposent et commercialisent dans l'UE des produits connectés ou des services liés à ces produits;
- détiennent des données pertinentes et les mettent à la disposition des destinataires de données situés dans l'UE;
- fournissent des services de traitement de données à des clients situés dans l'UE.

Ces entreprises doivent se conformer aux dispositions pertinentes du règlement.

Mesures déjà prises en Suisse

En Suisse, il n'existe actuellement aucune règle ou loi horizontale sur l'échange de données non personnelles entre personnes privées. Dans le domaine du droit public, la loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA, RS 172.019) contient des dispositions relatives à l'Open Government Data. Celles-ci ne s'appliquent toutefois qu'à l'administration fédérale. En réponse à la motion 22.3890 "Elaboration d'une loi-cadre sur la réutilisation des données" déposée par le Conseil des Etats, le Conseil fédéral a été chargé de créer les bases nécessaire afin que des infrastructures spécifiques permettant de réutiliser des données dans les domaines stratégiques soient rapidement développées et mises en place. L'OFJ a pris connaissance du Data Act dans le cadre de ses travaux législatifs habituels. Pour le moment, il n'a pas encore été décidé si et dans quelle mesure celui-ci sera intégré dans le projet.

Mesure 8

Espaces européens des données

Appellation complète de la mesure	Espaces européens des données
Type de mesure	Stratégie
Référence	-
Etat actuel	En cours de mise en œuvre
Date d'entrée en vigueur	-
Unité responsable dans l'administration fédérale	OFCOM/ChF

Description

La stratégie européenne pour les données (2020) définit la voie à suivre pour créer un véritable marché unique des données, dans lequel les données personnelles et non personnelles, y compris les données sensibles des entreprises, pourront circuler de manière transparente d'un pays à l'autre et entre les différents secteurs.

Concrètement, des espaces de données seront mis en place pour faciliter la mise en commun et le partage de données fiables et sécurisées dans des secteurs économiques stratégiques et des domaines publics. Les espaces de données européens seront progressivement interconnectés pour former un pilier du marché unique des données.

Des étapes importantes ont été franchies dans le **cadre législatif de l'UE pour les espaces de données**, notamment avec l'entrée en vigueur de la loi sur la gouvernance des données (voir mesure 6), l'adoption de la loi sur les données (voir mesure 7) et l'acte d'exécution sur les ensembles de données de grande valeur définis par la directive sur les données ouvertes._Massnahme_6_–_Massnahme_7_–

Depuis le lancement de la stratégie, la Commission européenne a annoncé 14 espaces de données dans des secteurs et domaines d'intérêt public différentes. Elle fournit une vue d'ensemble de l'état actuel des espaces de données européens communs dans un document de travail publié en janvier 2024. L'UE finance plusieurs initiatives liées aux espaces européens communs de données. Les actions de coordination et de soutien et les actions de déploiement sont principalement financées dans le cadre du programme Digital Europe, les initiatives d'innovation et de recherche dans le cadre du programme Horizon Europe.

Les espace européens des données existants sont les suivants:

1) **L'espace européen de données agricoles** renforcera la durabilité et la compétitivité de l'agriculture de l'UE grâce à la disponibilité et au partage des données sur la production, l'utilisation des terres, l'environnement et d'autres données.
2) **L'espace européen de données pour le patrimoine culturel** constitue l'initiative phare de la Commission pour accélérer la transformation numérique du secteur culturel européen et favoriser la création et la réutilisation du contenu du patrimoine culturel numérique.
3) **L'espace européen de données sur l'énergie** vise à consolider un cadre européen complet et cohérent pour le partage des données afin de soutenir des services énergétiques innovants, ce qui aidera l'UE à atteindre ses objectifs généraux en termes de sécurité énergétique, de durabilité et d'intégration des marchés de l'énergie (voir mesure 8b)._Massnahme_8b_–
4) **L'espace européen de données financières** contribuera à la transformation numérique du secteur financier de l'UE et à stimuler le secteur de la finance numérique en Europe.
5) **L'espace de données sur le pacte vert européen** soutiendra la mise en œuvre des politiques du Pacte vert à l'aide de données pertinentes (p. ex. sur la qualité de l'air, de l'eau et des sols dans le cadre de la stratégie zéro pollution) et contribuera à élever le niveau de protection de l'environnement.
6) **L'espace européen des données de santé** permettra aux personnes physiques de contrôler leurs données de santé électroniques tout en offrant aux chercheurs, aux innovateurs et aux décideurs politiques la possibilité d'utiliser ces données d'une manière sûre et fiable (voir mesure 8a)._Massnahme_8a_–

7) **L’espace européen de données industrielles** (manufacturières) aidera l'industrie manufacturière européenne à tirer davantage de valeur des données industrielles, à créer des chaînes d'approvisionnement plus souples et plus résistantes.
8) **L'espace européen de données linguistiques** vise à déployer un écosystème qui permette la collecte, la création, le partage et la réutilisation de données et de modèles linguistiques multimodaux dans tous les secteurs.
9) **L'espace européen de données sur les médias** vise à aider les organisations de médias à prospérer grâce à une collaboration fondée sur les données, et à relever les défis de l'économie numérique, notamment en ce qui concerne leur compétitivité sur un marché dominé par les plateformes en ligne.
10) **L'espace européen de données sur la mobilité** soutient les objectifs de la stratégie pour une mobilité durable et intelligente et facilite l'accès, la mise en commun et le partage des données provenant de sources de données existantes et futures sur les transports et la mobilité.
11) **L’espace de données des administrations publiques européennes** vise à favoriser le partage sécurisé des données destinées aux administrations publiques européennes.
12) **L’espace européen commun de données sur la recherche et l'innovation** a pour objectif d'approfondir les pratiques de la science ouverte en Europe.
13) **L'espace européen de données sur les compétences** offrira une infrastructure pour le partage, l'accès et la réutilisation des données relatives aux compétences et à l'éducation à des fins diverses, tels que le développement d'applications et de solutions innovantes, la modernisation de l'offre d'apprentissage, la recherche et l'analyse des tendances du marché du travail.
14) **L'espace européen de données sur le tourisme** répondra aux besoins des secteurs public et privé en matière de données et facilitera le partage, le traitement et l'analyse des données au sein du secteur. Pour les consommateurs, l’accès aux données permettra un choix parmi une meilleure offre. Pour les décideurs, il représentera un moyen de prévoir les mouvements de touristes et d'adapter les services publics en conséquence. Pour les entreprises, il permettra de mieux planifier et de mieux cibler leurs services.

Situation actuelle

Les espaces de données communs sectoriels sont mis en œuvre selon un calendrier qui leur est propre.

Possibles conséquences pour la Suisse

Les différents projets d'espaces européens de données ne concernent pas directement la Suisse. Cependant, dans tous les domaines, ces espaces pourraient contribuer à améliorer l'innovation et l'efficacité dans l'UE. Il pourrait être souhaitable que la Suisse puisse y accéder en fonction du domaine. En conséquence, l'interopérabilité des projets suisses avec les projets européens doit être assurée à un stade précoce. Ces travaux doivent également se poursuivre à partir de 2025 dans le cadre du point de contact à créer pour les espaces de données (sous la responsabilité de la Chancellerie fédérale, de l'OFCOM, de l'OFS et du DFAE DDIP).

En tant que membre du Système statistique européen (SSE) (accord sur les statistiques passé dans le cadre des négociations bilatérales II), la Suisse est indirectement concernée. La discussion sur les espaces de données, en particulier celui pour les statistiques, offrira certainement son lot d’opportunités et de risques au SSE.

Mesures déjà prises en Suisse

La Suisse aussi travaille intensivement sur les espaces de données. En décembre 2023, le Conseil fédéral a décidé de promouvoir un écosystème de données en Suisse et de gérer un point de contact pour les espaces de données à partir de 2025. De nombreux projets d'espaces de données sectoriels existent déjà ou sont en cours de réalisation, par exemple pour la santé (voir mesure 8a), l'énergie (voir mesure 8b), les transports publics, les géodonnées ou les statistiques. _Massnahme_8a_–_Massnahme_8b_–_Massnahme_8a_–_Massnahme_8b_–

Mesure 8a

Espace européen des données de santé

Appellation complète de la mesure	Règlement relatif à l'espace européen des données de santé
Type de mesure	Règlement
Référence	Proposition de règlement COM/2022/197 final
Etat actuel	Entrée en vigueur imminente
Date d'entrée en vigueur	Début 2025
Unité responsable dans l'administration fédérale	OFSP

Description

L'Espace européen des données de santé (European Health Data Space - EHDS) constitue un pilier important de l'Union européenne de la santé. Issu de la stratégie de l'UE en matière de données, il est le premier espace commun de données de l'UE consacré à un domaine spécifique. Le 3 mai 2022, la Commission européenne a publié une proposition de règlement relatif à l'espace européen des données de santé, laquelle a été adoptée par le Conseil le 15 mars 2024 et par le Parlement européen le 24 avril suivant.

L'EHDS vise à améliorer les soins de santé dans l'UE et à les préparer à l'avenir numérique. Il a comme objectif d'établir des règles claires ainsi que des normes et des infrastructures numériques communes pour faciliter l'utilisation des données de santé électroniques. Il doit servir aussi bien aux patients qu'à la recherche, à l'innovation, à la politique, à la sécurité des patients, aux statistiques et à des fins de réglementation.

L'EHDS comprend deux infrastructures numériques:

- **Utilisation primaire des données de santé:** Cette infrastructure permet l'échange de données de santé à des fins de soins directs aux patients (p. ex. dossiers médicaux et ordonnances électroniques). Elle a comme objectif de rendre les données accessibles par-delà les frontières, pour simplifier la prestation de services dans toute l'UE.
- **Réutilisation des données de santé:** Cette infrastructure vise à réutiliser les données de santé à des fins de recherche, d'innovation, de gestion de la politique et de réglementations. Un environnement cohérent doit être créé pour cela. _Massnahme_17_–

Quelques exemples concrets de fonctionnement:

- L'accès transfrontalier aux données des patients permet un traitement plus efficace à l'étranger.
- Pour des projets de recherche, des chercheurs peuvent avoir accès à de nombreuses données de santé, par exemple pour développer des outils basés sur l'IA.

L'EHDS se base sur les actes législatifs européens suivants:

- Règlement général sur la protection des données (RGPD)
- Règlement sur la gouvernance européenne des données (voir Mesure 6)_Massnahme_6_–
- Règlement sur les données (voir Mesure 7)_Massnahme_7_–
- Directive sur les réseaux et les systèmes d'information (voir Mesure 17)_Massnahme_17_–

La réussite du système EHDS repose notamment sur la confiance; il faut absolument que les citoyens puissent avoir confiance dans le fait que leurs données de santé sensibles seront protégées correctement et utilisées à bon escient. Le règlement prévoit les règles d'opt-out suivantes:

- Utilisation primaire: Les Etats membres peuvent proposer aux citoyens un opt-out pour les infrastructures à mettre en place dans le cadre du EHDS (p. ex. dossier du patient).

- Réutilisation: Des règles d'opt-out permettent de trouver un juste équilibre entre le respect des souhaits des patients et la garantie, dans l'intérêt public, de la disponibilité des bonnes données pour les bonnes personnes.

L'instauration du EHDS nécessite un travail important ainsi que des investissements financiers de la part des Etats membres. La Commission européenne apporte son soutien non seulement en cofinançant des initiatives telles que le projet pilote HealthData@EU, mais aussi par des aides financières directes aux Etats membres et par le développement des infrastructures existantes.

Situation actuelle

Le règlement relatif au EHDS a été adopté par le Conseil et le Parlement européens au printemps 2024. Il se trouve actuellement en cours de révision par les juristes-linguistes et devrait être publié début 2025 dans le Journal officiel de l'Union européenne. Il entrera en vigueur vingt jours après sa publication.

Dans un premier temps, l'utilisation primaire des données de santé doit progresser (début de l'échange de données à partir de 2028, puis extension à d'autres catégories de données en 2030). Les dispositions relatives à la réutilisation des données de santé doivent entrer en vigueur à partir de 2028. Pour certaines catégories de données (p. ex. données d'essais cliniques et données génétiques humaines), l'entrée en vigueur est prévue plus tard, en 2030.

Possibles conséquences pour la Suisse

Les possibilités de rattachement de pays tiers au système EHDS ne sont pas encore claires. L'UE souhaite d'abord compléter l'espace de données au sein de l'UE avant d'inclure les pays tiers. Actuellement, il reste important pour la Suisse de suivre de près les développements au niveau de l'UE.

Mesures déjà prises en Suisse

En Suisse, le programme national visant à promouvoir la transformation numérique du système de santé (DigiSanté) poursuit des objectifs comparables à ceux de l'EHDS. Il porte sur une mise en réseau numérique à grande échelle, sur l'interopérabilité entre les systèmes et les acteurs ainsi que sur l'amélioration de la disponibilité, de l'utilisation et de la qualité des données. Dans le cadre de quatre dispositifs de mise en œuvre, il est prévu de créer, de 2025 à 2034, les conditions préalables à la transformation numérique, d'établir les infrastructures nécessaires à un échange de données sûr et sans faille, d'améliorer encore les services de cyberadministration et les possibilités de réutilisation des données de santé pour la planification, le pilotage et la recherche. Le crédit d'engagement de 392 millions de francs déposé dans le cadre du programme a été approuvé par les deux Chambres fédérales au printemps 2024, ce qui permettra de lancer la mise en œuvre de DigiSanté dès 2025.

Depuis 2017, il existe par ailleurs en Suisse une base légale pour le dossier électronique du patient (DEP). Celui-ci doit renforcer la qualité du traitement médical, améliorer les processus de traitement, accroître la sécurité des patients et l'efficacité du système de santé et promouvoir les compétences des patients en matière de santé. La LDEP règle les conditions pour l'introduction et la diffusion du DEP. Elle fait actuellement l'objet d'une révision complète visant notamment à définir clairement la répartition des rôles entre la Confédération et les cantons en matière de DPE et à garantir le financement de celui-ci. Jusqu'à l'entrée en vigueur de la loi totalement révisée, le DEP sera amélioré constamment pour permettre le stockage de toutes les données utiles au traitement.

A l'occasion d'une initiative pour une infrastructure de recherche, la Confédération a en outre investi 135 millions de francs, de 2017 à 2024, dans le Swiss Personalized Health Network (SPHN) afin d'améliorer l'utilisation, pour la recherche biomédicale axée sur les données, des données de santé dont disposent les cinq hôpitaux universitaires suisses. De plus, le projet BioMedIT crée un Trusted Research Environment, à savoir un environnement informatique sécurisé pour la mobilisation, l'analyse et le stockage de données de recherche sensibles, qui peut être utilisé par tous les chercheurs suisses.

En réponse à la motion 22.3890 Elaboration d'une loi-cadre sur la réutilisation des données déposées par le Conseil des Etats, le Conseil fédéral a été chargé de créer les bases qui permettent de concevoir et d'instaurer rapidement, dans des domaines d'importance stratégique, des infrastructures spécifiques pour la réutilisation des données. L'OFJ a pris connaissance des travaux relatifs à l'EHDS dans le cadre de ses travaux législatifs

habituels. Pour le moment, il n'a pas encore été décidé si et à quel point les mesures de l'UE seront intégrées dans le projet de loi.

Les mesures décrites ont été lancées indépendamment des travaux relatifs à l'EHDS (interventions parlementaires et mandats du Conseil fédéral). La Suisse suit toutefois de près les développements relatifs à cet espace.

Mesure 8b

Espace européen des données sur l’énergie

Appellation complète de la mesure	Espace européen des données sur l’énergie
Type de mesure	Plan d’action/Communication
Référence	-
Etat actuel	
Date d’entrée en vigueur	
Unité responsable dans l’administration fédérale	OFEN

Description

Il convient de créer un espace européen commun de données sur l’énergie (European Energy Data Space - EEDS) fiable et sécurisé. Un tel espace a été annoncé dans la stratégie européenne en matière de données et dans le plan d'action de l'UE pour la transition numérique du système énergétique.

Cet espace de données vise à élargir l'accès aux données nécessaires au développement de services énergétiques innovants afin d'équilibrer et d'optimiser les réseaux électriques et d'améliorer l'efficacité énergétique de l'environnement bâti. Il jouera un rôle clé dans l'intégration des sources d'énergie renouvelables, faisant ainsi progresser les objectifs du paquet Fit for 55 et du plan RePowerEU.

L'espace de données sur l’énergie doit être étroitement lié aux espaces d’autres secteurs (p. ex. mobilité et communautés intelligentes) et permettre aux acteurs de différents secteurs, tels que la domotique et l'électromobilité, de participer activement au marché de l'énergie, de fournir des services énergétiques et de promouvoir l'intégration sectorielle (connexion des différentes sources d'énergie - électricité, chauffage, refroidissement, gaz, combustibles solides et liquides - entre elles et avec les secteurs d'utilisation finale tels que les bâtiments, les transports ou l'industrie). Ces acteurs pourront ainsi contribuer à une utilisation efficace de l'énergie, augmenter l'utilisation des énergies renouvelables, soutenir l'intégration, la coopération et l'échange d'informations entre différents secteurs, et créer de nouvelles possibilités commerciales. Plusieurs secteurs sont concernés, comme l'électricité, la domotique, l'électromobilité ou les communautés énergétiques.

Situation actuelle

Un appel d'offres pour la création d'un espace de données sur l’énergie à l'échelle de l'UE s’est clos le 29 mai 2024. Il a pour objectif de mettre en place une première version d'un espace européen commun de données sur l'énergie dans au moins dix Etats membres, d'identifier cinq cas d'utilisation (p. ex. gestion DER, services de flexibilité pour les réseaux électriques, recharge intelligente des véhicules électriques) et d'utiliser une architecture de référence commune reposant sur des normes ouvertes en matière d'interopérabilité des données. Il vise aussi l’élaboration de modèles commerciaux et l’instauration d'un système de gouvernance pour le suivi des opérations. Le projet a été attribué. Cependant, l’accord de financement sera signé que le 28 février 2025, on ne sait donc pas encore qui réalisera le projet.

Possibles conséquences pour la Suisse

L'idée de base d'un espace de données est de créer une infrastructure de données interopérable pour une multitude d'acteurs et de services situés à l’intérieur et à l’extérieur d'un secteur, basée sur des règles et des normes claires. La démarche comprend la définition de produits de données et de processus d'échange de données (voir l’étude Common European Energy Data Space). En tant que partie intégrante du système énergétique, un espace de données doit engendrer davantage de transparence, d’efficacité et d’opportunités commerciales grâce à une interopérabilité accrue et à un meilleur accès aux données, ce qui est profitable à la

société, à l'économie et aux autorités. On ne sait pas encore s'il sera possible de rattacher des pays tiers comme la Suisse à l'espace européen des données sur l'énergie. Actuellement, il reste important pour la Suisse de suivre de près les développements au niveau de l'UE.

En revanche, il ne fait aucun doute, au vu de la structure diversifiée et morcelée du secteur suisse de l'énergie, que la création d'un espace de données et un éventuel rattachement à l'espace européen correspondant vont donner lieu à quelques défis. En effet, les entreprises d'approvisionnement en énergie (EAE) suisses présentent par exemple un degré de numérisation très hétérogène, et les plus petites d'entre elles ne disposent que de peu de savoir-faire et de capacités en matière de standardisation des données.

D'un point de vue réglementaire, la loi révisée sur l'approvisionnement en électricité (partie de l'acte modificateur) contient déjà d'importantes exigences légales, qui peuvent faire office de bases pour un espace suisse des données sur l'énergie. Ainsi, l'harmonisation des données et l'amélioration de l'interopérabilité sont au cœur de la "plateforme de données", qui prévoit une connexion et donc une mise en réseau de tous les acteurs du marché suisse de l'électricité (et, à l'avenir probablement du gaz également). En outre, la même loi contient déjà des dispositions détaillées sur l'utilisation de la flexibilité (y compris les processus de recharge des véhicules électriques), dans la section relative à l'utilisation de systèmes de commande et de réglage intelligents. Ces compléments à la loi constituent toutefois une première étape dans la mise en œuvre des exigences et des mesures qu'impliqueraient l'adoption ou le rattachement de la Suisse à un espace européen des données sur l'énergie.

Mesures déjà prises en Suisse

Le rapport de fond de la Commission européenne (Common European Energy Data Space) cite plusieurs cas d'application que l'espace européen des données sur l'énergie devrait couvrir. Sont notamment mentionnés les centrales électriques virtuelles et l'agrégation, les processus de charge et de décharge sensibles aux prix sur les véhicules électriques et l'optimisation dans le domaine de l'énergétique des bâtiments.

Des études ont également identifié et examiné les cas d'application en Suisse. Smart Interoperability Architecture (SINA): the Decentralized Data Space in the Building Industry (terminée en avril 2024) et "Digitalisation dans le bâtiment - Interopérabilité et sécurité de l'information" (terminée en octobre 2022) font partie des études qui ont bénéficié d'un soutien ou d'un accompagnement.

La première a également analysé, du point de vue du secteur suisse, les possibles exigences liées à un espace européen de données sur l'énergie. Ainsi, dans l'optique d'un rattachement de la Suisse à l'espace européen de données, l'étude a constaté que "dans la mise en œuvre d'espaces de données (...), différentes lois doivent être respectées, notamment en ce qui concerne les questions de droit des données, comme le règlement général sur la protection des données (RGPD) de l'UE, ou la loi fédérale sur la protection des données (LPD). Le cadre établi par l'IDSA (International data spaces association) offre des solutions à cet égard, car il est conforme à la législation de l'UE en matière de protection des données et continuellement adapté aux modifications du droit. Il simplifie donc considérablement la mise en place et l'exploitation d'un espace de données en Suisse, où il faut toutefois tenir compte des spécificités de la LPD" (p. 8).

En outre, la faisabilité de réglementations techniques spécifiques dans le domaine des données de compteurs intelligents (Commission Implementing Regulation (EU) 2023/1162), l'accès aux données sur la flexibilité et leur échange (Network Code Demand Response) ont déjà été analysés. Cependant, peu de choses ont été faites au niveau de la mise en œuvre.

Mesure 9

Règlement européen sur les puces

Appellation complète de la mesure	Règlement établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs et modifiant le règlement (UE) 2021/694 (règlement sur les puces)
Type de mesure	Règlement
Référence	Règlement (UE) 2023/1781
Etat actuel	En vigueur
Date d'entrée en vigueur	21.09.2023
Unité responsable dans l'administration fédérale	SEFRI/SECO

Description

Le règlement européen sur les puces (European Chips Act) est entré en vigueur le 21 septembre 2023 (règlement (UE) 2023/1781). L'UE souhaite ainsi renforcer sa compétitivité dans les technologies des semi-conducteurs et réduire sa dépendance en matière d'approvisionnement. Le règlement fixe cinq objectifs:

- Augmenter les capacités de production de 10% à 20% d'ici 2030
- Renforcer le leadership européen en matière de recherche et de technologie
- Renforcer les capacités et le leadership en matière de conception, de production et de commercialisation
- Développer les connaissances relatives aux chaînes d'approvisionnement mondiales
- Remédier à la pénurie de main-d'œuvre qualifiée, attirer et promouvoir les talents

Le règlement a été publié dans le cadre d'un paquet plus large comprenant trois piliers principaux:

- Initiative Chips for Europe (Pilier1): Renforcer les capacités technologiques et l'innovation en comblant le fossé entre les capacités avancées de recherche et d'innovation et leur exploitation industrielle.
- Cadre pour la sécurité d'approvisionnement (Pilier 2): Créer un cadre visant à garantir la sécurité d'approvisionnement et la résilience du secteur des semi-conducteurs en attirant les investissements et en renforçant les capacités de production dans les secteurs de la fabrication, de l'emballage, des essais et de l'assemblage. Il doit être plus facile pour les Etats membres de l'UE d'accorder des aides aux sites de production qui obtiennent le statut d'"installation de production intégrée ou de fonderie ouverte de l'UE"[1]. L'Allemagne a par exemple annoncé vouloir soutenir Intel, SMC, Wolfsspeed et Bosch à hauteur de 4.8 milliards d'euros[2].
- European Semiconductor Board (ESB) (Pilier 3): Création d'un mécanisme de coordination entre les Etats membres de l'UE et la Commission pour renforcer le suivi et la gestion des crises. L'ESB assure également la supervision de l'European Chips Act.

Le règlement européen sur les puces prévoit de mobiliser plus de 43 milliards d'euros d'investissements publics et privés d'ici 2030. Les dépenses proposées dans le cadre de l'initiative Chips for Europe seront alimentées par des budgets déjà existants dans le cadre d'Horizon Europe et du DEP, complétés par des investissements nationaux et par des investissements privés à long terme.

Le règlement européen sur les puces s'ajoute à d'autres initiatives dans le domaine des semi-conducteurs, telles que l'alliance de l'industrie des semi-conducteurs, les activités de programme dans ce domaine (p. ex. entreprise commune ou dans le cadre d'Horizon Europe ou du DEP, le "projet important d'intérêt européen commun" (IPCEI)

[1] Voir le projet de document d'orientation p.9 (Règlement européen sur les semi-conducteurs: La Commission publie des orientations sur la procédure de demande de statut d'installation de production intégrée et de fonderie ouverte de l'UE | Bâtir l'avenir numérique de l'Europe (europa.eu)

[2] BMWK - Le fonds pour le climat et la transformation 2024: créer un allègement, garantir les investissements d'avenir, organiser la transformation

dans le domaine de la microélectronique et des technologies de communication, ou les aides d'Etat au titre de la facilité pour la reprise et la résilience (FRR).

Situation actuelle

Le règlement a été publié au Journal officiel de l'UE le 18 septembre 2023 et est en vigueur depuis le 21 septembre 2023.

Possibles conséquences pour la Suisse

L'European Chips Act s'inscrit principalement dans le contexte des tensions entre la Chine et Taïwan et est largement motivé par des ambitions géopolitiques. Comme pour d'autres initiatives actuelles de l'UE en matière de politique industrielle, des effets économiques tant positifs que négatifs sont possibles. Ainsi, les programmes ouvrent en partie de nouveaux débouchés aux fournisseurs et aux producteurs suisses. En outre, l'industrie pourrait bénéficier de possibilités d'approvisionnement plus diversifiées. D'autre part, les subventions peuvent fausser la concurrence au détriment des producteurs. Cela vaut également pour l'industrie suisse des semi-conducteurs, active dans le monde entier, qui est très diversifiée en termes de taille et de spécialisation tout au long de la chaîne de création de valeur.

Pour mettre en œuvre l'initiative Chips for Europe, le European Chips Act prévoit notamment la création d'une entreprise commune pour les semi-conducteurs (Chips JU) dotée d'un budget de 4,2 milliards (2021-2027) et financée par Horizon Europe et le DEP. L'objectif déclaré du Conseil fédéral reste l'association la plus rapide possible au paquet Horizon afin d'offrir aux acteurs de la recherche en Suisse les meilleures conditions pour participer aux activités européennes. D'une manière générale, la Suisse s'engage à ce que les initiatives prises à l'étranger ne comportent pas d'éléments protectionnistes et à ce que les programmes d'encouragement et de recherche soient, dans la mesure du possible, ouverts aux pays tiers. En octobre 2023, la Commission a présenté une liste de domaines technologiques considérés comme critiques pour la sécurité économique de l'Union européenne, dont les technologies des semi-conducteurs. Une conséquence immédiate est que les chercheurs suisses, même s'ils sont éventuellement associés à Horizon-Europe et au DEP, seront probablement touchés par des restrictions dans leur collaboration avec l'Europe.

Mesures déjà prises en Suisse

Le 24 mai 2023, le Conseil fédéral a adopté des mesures transitoires afin d'atténuer les effets dus à l'exclusion des acteurs suisses des domaines considérés comme stratégiques par l'Europe. Sur cette base, le SEFRI a lancé une mesure transitoire dans le secteur des semi-conducteurs, qui s'adresse en premier lieu aux centres de recherche universitaires suisses. L'initiative SwissChips correspondante, dotée d'une somme d'encouragement maximale de 26 millions de francs, est harmonisée avec les activités européennes prévues et s'appuie en même temps sur les points forts de la Suisse dans la recherche sur les semi-conducteurs.

Le 13 juin 2024, le Conseil national a adopté le postulat Cottier 23.3866, qui demande une stratégie suisse pour les semi-conducteurs. En réponse à ce postulat, le Conseil fédéral analysera les effets des mesures de politique industrielle étrangères dans le domaine des semi-conducteurs (y compris celles de l'UE) et examinera également les possibilités d'améliorer les conditions-cadres.

Mesure 10

Stratégie européenne pour une technologie quantique

Appellation complète de la mesure	Stratégie européenne pour une technologie quantique
Type de mesure	Stratégie
Référence	-
Etat actuel	En cours de mise en œuvre
Date d'entrée en vigueur	29 octobre 2018
Unité responsable dans l'administration fédérale	SEFRI

Description

En octobre 2018, la Commission européenne a lancé l'initiative Quantum Technologies Flagship, qui rassemble des établissements de recherche, le secteur privé et des fonds publics afin de promouvoir les technologies quantiques en Europe. Elle durera jusqu'en 2028 et soutiendra des projets du domaine quantique pour un montant total d'un milliard d'euros. Etabli le 3 mars 2021, l'agenda de recherche stratégique (*Strategic Research Agenda*, SRA) du Flagship, définit une orientation claire pour le développement de la recherche et de l'innovation dans ce domaine. Dans le cadre du Quantum Flagship, la recherche et l'innovation se concentrent sur quatre domaines :

i. **la communication quantique** pour le développement de réseaux capables de transmettre en toute sécurité des volumes croissants de données;
ii. **les calculateurs quantiques**, pour fournir une capacité de calcul monumentale afin de résoudre des problèmes complexes;
iii. **la simulation quantique** de phénomènes non linéaires complexes ou de processus microscopiques au niveau moléculaire ou atomique (p. ex. météo, processus chimiques ou atomiques),
iv. **les capteurs et mesures quantiques,** pour des résultats de mesure exacts. L'agenda du *Quantum* Flagship doit mettre en œuvre ces quatre priorités par les mesures suivantes:
    1. implication de tous les acteurs importants du secteur, création d'un milieu innovant;
    2. promotion de l'**accès au financement,** construction d'une industrie quantique durable en Europe;
    3. création de l'**infrastructure et des chaînes de création de valeur**, élaboration de normes industrielles avec des partenaires internationaux;
    4. élaboration d'une stratégie européenne en matière de **propriété intellectuelle et définition de normes** (en collaboration avec l'Office européen des brevets);
    5. **formation et relations publiques**, promotion de l'enseignement de la physique quantique, formation et encouragement des spécialistes.

Situation actuelle

La mesure est en vigueur depuis le 29 octobre 2018. Les premiers projets dans les domaines susmentionnés ont commencé conformément au SRA. La deuxième phase de l'initiative Quantum Flagship a démarré avec les appels d'offres lancés dans le cadre du programme Horizon Europe. Elle a pour but de renforcer le rôle de leadership européen en matière de recherche dans le domaine des technologies quantiques et de rapprocher les résultats de la recherche de l'exploitation industrielle. Le Programme pour une Europe numérique fournira un financement supplémentaire lié aux technologies quantiques et destiné au développement ainsi qu'au renforcement des capacités numériques stratégiques de l'Europe.

Possibles conséquences pour la Suisse

Ces dernières années, en Suisse, les chercheurs ont participé avec succès à des projets de technologie quantique dans le cadre d'Horizon 2020/Quantum Technologies Flagship et de QuantERA. La Suisse est intéressée à poursuivre sa coopération de longue date avec l'Europe dans ce domaine. Cependant, l'association à Horizon

Europe et à Digital Europe étant une condition préalable pour que la Suisse continue à participer aux différentes activités dans le domaine des technologies quantiques, elle est restée exclue jusqu'à la fin de l'année 2024. Les négociations pour une association étant conclues le 20 décembre 2024, un arrangement transitoire a été activé, qui permet aux chercheurs et innovateurs suisse de participer à la plupart des appels sous Horizon Europe et Digital Europe. La participation à quelques appels de haut TRL dans le domaine quantique est soumise à des conditions supplémentaires.

La souveraineté technologique étant l'une des priorités de la stratégie numérique de l'UE, les pays tiers associés à Horizon Europe et au Digital Europe Programme risquent fort, malgré les accords d'association, de se voir exclus de certains domaines technologiques sensibles, tels que les technologies quantiques. L'UE travaille actuellement à l'élaboration et à l'instauration d'une infrastructure de communication quantique (EuroQCI) afin d'intégrer les technologies quantiques dans les infrastructures de communication conventionnelles et de permettre ainsi une transmission ultra-sécurisée des données. Pour des raisons de souveraineté technologique, elle a exclu la participation de pays tiers comme la Suisse. Même si la Suisse est associée aux programmes Horizon Europe et Digital Europe Programme, il se peut qu'elle soit tout de même exclue de certaines activités (p. ex. la construction et l'acquisition d'ordinateurs quantiques ou d'infrastructures de communication quantiques).

Mesures déjà prises en Suisse

Le Conseil fédéral a décidé de renforcer la Suisse en tant que pôle de recherche par des mesures transitoires.

Le Conseil fédéral prévoit des mesures supplémentaires dans les domaines de recherche d'importance stratégique pour la Suisse, comme la recherche quantique. Elles ont pour objectif de renforcer structurellement et durablement la recherche en Suisse. Elles sont complémentaires au programme-cadre de l'UE et à une association de la Suisse. Dans ce contexte, le Conseil fédéral a décidé, en mai 2022, de lancer la Swiss Quantum Initiative (SQI).

La Suisse renforce par ailleurs sa stratégie de coopération internationale dans le domaine de la technologie quantique (p. ex. participation à la nouvelle Table ronde internationale sur la recherche commune en matière d'information quantique) ainsi que les accords bilatéraux conclus avec des partenaires prioritaires.

Mesure 11

Règlement EuroHPC

Appellation complète de la mesure	Règlement établissant l'entreprise commune pour le calcul à haute performance
Type de mesure	Règlement
Référence	Règlement (UE) 2021/1173
Etat actuel	En vigueur
Date d'entrée en vigueur	13.07.2021
Unité responsable dans l'administration fédérale	SEFRI

Description

Avec le cadre financier pluriannuel (CFP) pour la période 2021-2027, la Commission européenne (COM) a décidé de réviser le règlement de l'entreprise commune européenne pour le calcul haute performance (GU EuroHPC) (règlement UE 2021/1173), qui sera désormais un partenariat institutionnel. Les participants à l'entreprise commune EuroHPC sont les Etats membres de l'UE, les Etats associés à Horizon Europe, à Digital Europe et/ou à l'instrument de financement de l'UE Connecting Europe Facility (CEF), ainsi que les associations privées European Technology Platform for High Performance Computing (ETP4HPC) et Big Data Value Association (BDVA). Le règlement proposé le 18 septembre 2020 prévoit pour l'essentiel la poursuite de l'initiative existante, avec les tâches principales suivantes :

1. **Infrastructure** : Acquérir une infrastructure de calcul et de données à haute performance de classe mondiale (y compris les futurs ordinateurs quantiques) et moderniser l'infrastructure actuelle. Plusieurs supercalculateurs ont déjà été acquis (p. ex. l'infrastructure LUMI en Finlande, à laquelle la Suisse participe).
2. **Fédération des services de calcul haute performance :** Garantir aux utilisateurs publics et privés de toute l'Europe un accès, à l'échelle de l'Union et basé sur le cloud, à des ressources groupées et sécurisées en matière de calcul à haute performance, d'informatique quantique et de données.
3. **Technologie :** Soutenir un programme de recherche et d'innovation visant à développer un écosystème européen de supercalcul de niveau mondial.
4. **Application :** Soutenir les activités visant à maintenir la position dominante de l'Europe dans le développement d'applications de calcul et de données ainsi que de codes logiciels importants pour la science, l'industrie (y compris les PME) et le secteur public.
5. **Développement de l'utilisation et des compétences :** Créer et mettre en réseau des centres de compétences nationaux en matière de HPC afin de promouvoir l'utilisation scientifique et industrielle des ressources de supercalcul et des applications de données.

En juillet 2021, le règlement GU EuroHPC a été adopté. Il définit une mission ambitieuse, avec un budget nettement supérieur pour la période 2021-2027, à savoir 7 milliards d'euros, dont 1.9 milliard issu du programme Europe numérique (DEP), 900 millions d'Horizon Europe et 200 millions de la facilité Connecting Europe. La contribution des Etats participants est équivalente, tandis que celle des membres privés s'élève à 900 millions d'euros (en nature et en espèces). Aujourd'hui, six superordinateurs cofinancés par EuroHPC sont pleinement opérationnels: LUMI en Finlande (5e rang mondial[3]), LEONARDO en Italie (7e), MareNostrum 5 en Espagne (9e), Vega en Slovénie, MeluXina au Luxembourg, Discoverer en Bulgarie, Karolina en République tchèque et Deucalion au Portugal. EuroHPC a également annoncé cinq nouveaux sites d'hébergement pour une nouvelle génération de superordinateurs européens en Allemagne, en Grèce, en Hongrie, en Irlande et en Pologne.

Le 24 janvier 2024, la Commission a proposé une modification de l'actuel règlement EuroHPC (UE 2021/1173) du Conseil de 2018 afin d'y inclure une autre tâche essentielle, à savoir la conception et l'exploitation d'"usines d'IA" pour soutenir le développement d'un écosystème d'IA hautement compétitif et innovant dans l'Union. Les capacités de calcul haute performance de l'Union pourraient ainsi être mises à la disposition de start-ups

[3] Tiré de TOP500, la liste des superordinateurs les plus rapides du monde (TOP500 List - June 2024 | TOP500)

européennes innovantes pour la formation et le réglage fin des modèles (notamment linguistiques) de l'IA les plus avancés. La modification proposée s'inscrit dans le cadre de l'initiative de l'Union en matière d'IA, annoncée par la présidente de la Commission, Ursula von der Leyen, dans son discours sur l'Etat de l'Union 2023. Le règlement portant modification a été adopté au Conseil COMPET Recherche le 23 mai 2024.

Situation actuelle

La modification relative à l'IA est entrée en vigueur le 9 juillet 2024. Des appels à projets seront publiés par EuroHPC.

Possibles conséquences pour la Suisse

La Suisse joue un rôle de pionnier en Europe dans le domaine du calcul haute performance. Le supercalculateur Piz Daint du Centre suisse de calcul scientifique (CSCS), à Lugano, comptait déjà parmi les plus puissants du monde en 2013, et son successeur Alps occupe le 6e rang mondial depuis juin 2024.

La Suisse, qui était membre à part entière de l'entreprise commune EuroHPC depuis mars 2019, souhaitait poursuivre son excellente collaboration avec l'UE dans le domaine du calcul haute performance. Or, comme EuroHPC a été intégré à Digital Europe et qu'une association à Horizon Europe ou à Digital Europe constitue une condition préalable à la participation aux différentes activités d'EuroHPC, la Suisse est actuellement exclue.

Pour la stratégie suisse, les récents événements sont problématiques:

a. La Suisse ne peut plus participer à la conception de grands projets communs d'infrastructure HPC à l'échelle européenne. Sa participation à l'infrastructure LUMI en Finlande était cruciale pour elle, du point de vue scientifique autant qu'économique (problème de l'explosion des prix de l'électricité).
b. La collaboration dans le domaine des applications, par exemple en matière de simulation météorologique/climatique, ou la participation aux différents centres d'excellence européens dans le domaine du HPC, ne sont désormais plus possibles. L'exclusion des communautés correspondantes empêche de réaliser les avancées technologiques nécessaires.

En raison du cycle de vie court des systèmes HPC et compte tenu de la nouvelle modification du règlement relative à l'IA, laquelle prévoit la mise à disposition de ressources supplémentaires d'IA, il est souhaitable que la Suisse devienne membre d'EuroHPC dans un avenir proche. Cela sera possible après la signature de l'accord d'association aux programmes UE avec l'application provisoire de l'accord. L'arrangement transitoire permet déjà une participation aux appels de projet et un statut d'observateur dans le partenariat.

Mesures déjà prises en Suisse

Après la non-association de la Suisse à Horizon Europe et à Digital Europe, le SEFRI a pris les premières mesures. L'initiative SwissTwins a été lancée fin 2022 sous la direction de l'EPFZ, avec pour objectif la mise à disposition d'une plateforme intégrée pour la simulation météorologique/climatique sur le nouveau supercalculateur Alps à Lugano. Indépendamment de cela, le domaine des EPF a lancé la SWISS AI Initiative, qui poursuit des objectifs similaires à ceux du règlement européen.

Mesure 12

Echange électronique d'informations sur la sécurité sociale

Appellation complète de la mesure	Echange électronique d'informations sur la santé sociale (EESSI)
Type de mesure	Projet de numérisation
Référence	EESSI
Etat actuel	En cours de mise en œuvre
Date d'entrée en vigueur	05.07.2019
Unité responsable dans l'administration fédérale	OFAS

Description

L'Echange électronique d'informations sur la sécurité sociale (*Electronic Exchange of Social Security Information* - EESSI) découle de deux règlements européens de coordination des systèmes nationaux de sécurité sociale (règlement (CE) No. 883/2004 et règlement (CE) No. 987/2009), que la Suisse a repris dans le cadre de l'accord sur la libre circulation des personnes entre la Suisse et l'UE, ainsi que dans la Convention de l'Association européenne de libre-échange (AELE).

L'EESSI est un système informatique décentralisé qui interconnecte environ 3 400 institutions de sécurité sociale dans les 32 pays qui y participent, à savoir les 27 Etats membres de l'UE, l'Islande, le Liechtenstein, la Norvège, le Royaume-Uni et la Suisse. Les composants du système ont été financés, développés et livrés par la Commission européenne (COM).

Grâce à l'EESSI, les institutions de sécurité sociale de ces pays échangent de manière rapide et sécurisée, via des points d'accès nationaux, des informations relatives aux différentes branches de la sécurité sociale (chômage, famille, pension, prestations de maladie et de maternité/paternité, accidents du travail, recouvrement et législation applicable). Ces échanges contribuent à améliorer la protection des droits des citoyens en matière de sécurité sociale au-delà des frontières. L'EESSI constitue donc un pilier important de la libre circulation des personnes en Europe.

Situation actuelle

Il était prévu que l'EESSI entre en fonction en 2012, mais la complexité du système a ralenti le projet au point que le déploiement n'a démarré qu'au mois de juillet 2019 et qu'il devrait se poursuivre jusqu'en 2025.

Sur les 32 pays participants à l'EESSI, 19 (AT, BG, DE, EE, HU, IS, LV, MT, SE, UK, CY, DK, NO, PT, FR, IE, LI, FI, LT) ont totalement terminé l'intégration du système. Le projet pourra être clôturé lorsque les autres pays, dont la Suisse, auront eux aussi terminé le déploiement, en principe courant 2025. La phase de déploiement et la maintenance évolutive du système sont donc menées de front, ce qui sollicite de nombreuses ressources, dans tous les pays concernés.

A la fin de l'année 2020, la COM a transféré unilatéralement, et sans consultation préalable, la responsabilité de la maintenance évolutive de certains composants aux pays participants à l'EESSI (HandOver). Depuis, l'OFAS (Office fédéral des assurances sociales) et l'OFIT (Office fédéral de l'informatique et de la télécommunication) garantissent conjointement le bon fonctionnement du système en Suisse.

Possibles conséquences pour la Suisse

Les règlements européens de coordination des systèmes de sécurité sociale sont directement applicables à la Suisse. Toutes les institutions d'assurances sociales suisses sont aujourd'hui directement ou indirectement connectées à l'EESSI et échangent de l'information avec les autres institutions en Europe.

Le financement de la partie suisse du système est assuré par le prélèvement d'émoluments auprès des institutions suisses utilisatrices.

D'autres éléments à venir auront un des conséquences significatives sur l'EESSI et son fonctionnement, et par conséquent aussi sur les citoyens et les institutions suisses de sécurité sociale, en particulier l'initiative ESSPASS (voir mesure 13), étroitement liée à l'identité numérique et portefeuille électronique européen (EUID-Wallet), donc à eIDAS (voir mesure 5). Massnahme 5 –

Mesures déjà prises en Suisse

Pour des volumes d'échanges importants, le développement d'applications ad hoc s'impose, comme cela a été le cas dans le domaine des pensions du premier pilier (développement et maintenance auprès de la Centrale suisse de compensation) et dans le cadre de la détermination de la législation de sécurité sociale applicable aux personnes (développement et maintenance auprès de l'OFAS), ainsi que dans le cadre de l'assurance-maladie (développement et maintenance auprès de l'Institution Commune LAMal).

Mesure 13

Passeport européen de sécurité sociale

Appellation complète de la mesure	Passeport européen de sécurité sociale (ESSPASS)
Type de mesure	Initiative
Référence	ESSPASS
Etat actuel	Phase pilote
Date d'entrée en vigueur	A déterminer
Unité responsable dans l'administration fédérale	OFAS

Description

Le plan d'action du pilier européen sur le socle européen des droits sociaux a prévu le lancement de l'initiative du passeport européen de sécurité social (*European Social Security Pass* - ESSPASS), conçue dans le but de chercher, par le biais d'activités pilotes, une solution numérique pour l'émission et la vérification transfrontalière des documents de sécurité sociale (à savoir les documents portables délivrés aux citoyens pour faire valoir leurs droits en Europe en matière de sécurité sociale, p. ex. la carte européenne d'assurance maladie; *European Health Insurance Card*).

L'ESSPASS s'inscrit dans les règlements européens de coordination des systèmes nationaux de sécurité sociale (règlement (CE) No. 883/2004 et règlement (CE) No. 987/2009), et concerne les 32 pays qui les appliquent (dont la Suisse).

Alors que l'EESSI (voir mesure 12) ne permet des échanges numérisés qu'entre les institutions de sécurité sociale, l'ESSPASS prévoit d'aider les personnes qui voyagent ou se déplacent dans un autre pays ainsi que les entreprises qui exercent des activités à l'étranger à interagir numériquement avec les institutions de sécurité sociale, d'autres organismes publics tels que les inspecteurs du travail, ou des prestataires de soins de santé, chaque fois que cela est nécessaire. _Massnahme_12_–

Etroitement lié à l'identité numérique, l'ESSPASS a pour objectif la création et l'échange de documents numériques nécessaires à la coordination des systèmes de sécurité sociale. Il vise donc à permettre leur émission, la vérification de leur authenticité et de leur validité en temps réel, ainsi que de leur traçabilité, tout en réduisant les obstacles administratifs et le risque d'erreurs et de fraudes.

L'ESSPASS est indépendant de toute technologie, et vise l'exploration et l'identification de la meilleure solution, compte tenu de toutes les exigences et des spécificités nationales. A cet égard, il s'appuie sur d'autres initiatives de l'Union européenne, en particulier:

- le règlement relatif au **portail numérique unique** (règlement (EU) 2018/1724). Le site internet Your Europe fournit un point d'entrée unique pour les citoyens et les entreprises qui souhaitent demander la numérisation des documents de coordination de la sécurité sociale dans le cadre du règlement sur le portail numérique unique;
- le cadre de **l'identité numérique de l'UE** (EUID, voir mesure 5) pour permettre aux personnes et aux entreprises de s'identifier et de stocker dans leur portefeuille électronique (EUID-Wallet) les documents relatifs aux droits en matière de sécurité sociale; _Massnahme_5_–
- l'infrastructure européenne des services de chaînes de blocs (*European Blockchain Services Infrastructure* - EBSI, voir mesure 23), qui vise à tirer parti de la blockchain pour créer des services transfrontaliers destinés aux administrations publiques, aux citoyens et à leurs écosystèmes, afin de vérifier les informations et de rendre les services dignes de confiance._Massnahme_23_–

Situation actuelle

L'initiative ESSPASS a débuté en 2021 par une première phase d'activités pilotes, lancée par la DG EMPL (direction générale de l'emploi, des affaires sociales et de l'inclusion) et l'organisme italien de sécurité sociale (*Istituto Nazionale della Previdenza Sociale - INPS*) et qui s'est concentrée sur la numérisation des procédures pour le document blockchain. Treize autres Etats membres de l'UE ont suivi les activités, la plupart du temps en tant qu'observateurs.
Dans le prolongement de cette première phase d'activités pilotes ESSPASS, deux consortiums, DC4EU et EBSI Vector, poursuivent l'expérimentation de la délivrance et de la vérification du document portable A1 et de la Carte européenne d'assurance maladie. Ils devraient rendre leurs rapports et présenter leurs travaux d'ici la fin du premier semestre 2025.

Selon la communication de la Commission européenne (COM) de septembre 2023 sur la numérisation de la coordination de la sécurité sociale (COM [2023] 501 final), il convient, à la lumières des résultats des activités pilotes menées par les consortiums, de décider des prochaines étapes, notamment de la possibilité de déployer une solution ESSPASS dans tous les pays de l'UE et de la nécessité d'un cadre législatif.

Possibles conséquences pour la Suisse

Les citoyens européens au bénéfice de documents portables numérisés pourront faire valoir leurs droits en matière de sécurité sociale lors d'un séjour temporaire en Suisse. Les autorités et les organismes suisses concernés devront alors être en mesure de lire ce nouveau type de documents; ils ne pourront pas exiger qu'un document physique leur soit présenté. Cela représentera assurément un défi pour les prestataires de soins de santé.

Lorsque l'infrastructure de confiance prévue par le projet de loi sur l'e-ID sera disponible en Suisse et compatible avec celle de l'UE, les institutions suisses pourront émettre de tels documents portables numériques parallèlement à des documents portables physiques. Cela permettra aux citoyens suisses de faire valoir leurs droits en matière de sécurité sociale lors de leurs séjours en Europe.

En Suisse, la carte européenne d'assurance maladie figure au verso de la carte d'assuré suisse; celle-ci devra s'adapter à la numérisation de celle-là.

Mesures déjà prises en Suisse

L'OFJ, fedpol et l'OFIT œuvrent d'ores et déjà à la création de l'infrastructure de confiance telle que prévue par le projet de loi sur l'e-ID en Suisse (eID, wallet, registres, etc) compatible avec celle de l'UE.

L'OFAS participe activement aux travaux du consortium DC4EU (consortium pour les justificatifs numériques pour l'Europe), et coordonne les travaux avec les potentiels acteurs en Suisse pour un pilote à large échelle, à savoir l'OFSP, Santésuisse via Sasis AG pour l'émission de la carte européenne d'assurance maladie d'une part, et le SECO, la Caisse fédérale de compensation AVS et l'inspectorat du travail du canton du Tessin pour l'émission de l'attestation d'assujettissement A1. L'OFAS se prépare par ailleurs à la mise en place des systèmes de lecture de ces nouveaux documents.

Mesure 14

Règlement sur les infrastructures gigabit

Appellation complète de la mesure	Règlement sur les infrastructures gigabit
Type de mesure	Règlement
Référence	Règlement (UE) 2024/1309
Etat actuel	En vigueur
Date d'entrée en vigueur	11.05.2024
Unité responsable dans l'administration fédérale	OFCOM

Description

Le règlement relatif à des mesures visant à réduire le coût du déploiement de réseaux gigabit de communications électroniques (Gigabit Infrastructure Act, GIA) est entré en vigueur le 11 mai 2024. Il vise à accélérer le déploiement de réseaux à haut débit tels que la fibre optique et la 5G, et à stimuler les investissements dans l'infrastructure numérique. En outre, sur proposition du Parlement européen, il a intégré la suppression des frais de communication intra-UE.

S'agissant d'accélérer le déploiement du réseau, les procédures d'autorisation doivent notamment être simplifiées. Le règlement oblige les Etats membres à instaurer une autorité nationale pouvant traiter certains litiges entre les pouvoirs publics et les opérateurs de télécommunications et prendre des décisions contraignantes en vue de leur règlement. Il introduit en outre le principe du *tacit-approval*, selon lequel une demande d'extension de réseau est considérée comme tacitement approuvée si l'autorité compétente n'a pas répondu dans un délai donné. Le Parlement et le Conseil ont trouvé un compromis et fixé le délai de réponse à quatre mois. Les Etats membres peuvent toutefois déroger entièrement au principe de l'approbation tacite, soit en obligeant leurs autorités à indemniser les demandeurs si aucune réponse n'a été fournie dans les délais, soit en accordant aux demandeurs le droit d'intenter une action en justice. Par ailleurs, l'installation de la fibre optique sera obligatoire dans tous les bâtiments neufs ou rénovés pour lesquels des permis de construire auront été demandés après le 12 février 2026. Des exceptions sont prévues pour les infrastructures nationales critiques.

Situation actuelle

Les frais de communication intra-UE seront supprimés d'ici 2029. Actuellement, les habitants de l'UE ne paient pas de frais d'itinérance lorsqu'ils voyagent à l'intérieur de l'UE, mais des frais leur sont facturés lorsqu'ils passent un appel ou envoient un SMS depuis leur pays d'origine vers un autre Etat membre. Les plafonds tarifaires actuellement fixés (0,19€/min pour les appels et 0,06€/SMS) pour les communications intra-UE ont expiré en mai 2024 et sont prolongés jusqu'au 1er janvier 2032 en vertu du nouveau règlement du 14 mai 2024. Au plus tard le 30 juin 2027, la Commission doit présenter une analyse d'impact concernant la suppression progressive du plafond tarifaire. D'ici juin 2028, elle doit adopter un acte d'exécution pour supprimer les frais de communication intra-UE, de sorte qu'à partir du 1er janvier 2029, les prix de détail correspondront aux prix nationaux.

Possibles conséquences pour la Suisse

Il n'y a pas de conséquences directes pour la Suisse.

Mesures déjà prises en Suisse

Indépendamment du Gigabit Infrastructure Act, le Conseil fédéral a chargé le DETEC d'élaborer un projet de consultation pour une stratégie Gigabit en Suisse.

Mesure 15

Stratégie de cybersécurité

Appellation complète de la mesure	Stratégie de cybersécurité de l'UE
Type de mesure	Stratégie
Unité responsable dans l'administration fédérale	OFCS/DFAE ADIGI/DFAE AIS

Description

La Communication sur "La stratégie de cybersécurité de l'UE pour la décennie numérique" du 16 décembre 2020 propose d'intégrer la cybersécurité dans chacun des maillons de la chaîne d'approvisionnement et de rassembler les activités et ressources de l'UE dans les quatre communautés de cybersécurité - marché intérieur, services répressifs, diplomatie et défense. La stratégie couvre la sécurité des services essentiels tels que les hôpitaux, les réseaux d'énergie, les chemins de fer et le nombre toujours croissant d'objets connectés dans les maisons, bureaux et usines. Elle vise à mettre en place des capacités collectives pour répondre à des cyberattaques majeures. Elle expose également des plans visant à collaborer avec des partenaires du monde entier pour assurer la sécurité et la stabilité internationales dans le cyberespace. La stratégie contient des mesures liées à trois domaines d'action de l'UE: 1) la résilience, la souveraineté technologique et le leadership; 2) la capacité opérationnelle de prévention, de dissuasion et de réaction; et 3) la coopération pour faire progresser un cyberespace mondial et ouvert. Durant cette législature, plusieurs législations ont été adoptées qui mettent en œuvre cette stratégie (voir mesures 16, 17, 18 et 19).

Lors de la réunion des ministres des télécommunications du 21 mai 2024, le Conseil européen a adopté des conclusions sur le futur de la cybersécurité. Celles-ci demandent la révision de la stratégie de l'UE en matière de cybersécurité de 2020 et l'actualisation de ses objectifs et son approche, par la définition d'un cadre clair qui prévoie des rôles et des responsabilités pour toutes les entités concernées, des mécanismes de coordination simples et efficaces et une coopération renforcée avec le secteur privé et le monde universitaire. Le Conseil invite par conséquent la Commission et le Haut représentant de l'UE pour les affaires étrangères et la politique de sécurité à évaluer les résultats et les lacunes de la stratégie actuelle ainsi que ses conséquences, et à présenter sur cette base une stratégie révisée.

La mise en œuvre de la stratégie de cybersécurité est soutenue par des appels d'offres dans le cadre des programmes Horizon Europe et Digital Europe.

Situation actuelle

La "Stratégie de cybersécurité de l'UE pour la décennie numérique", publiée le 16 décembre 2020, n'est pas un document législatif mais plutôt un cadre stratégique. En tant que tel, elle n'entre pas en vigueur à une date précise, contrairement à une directive ou un règlement. Cependant, elle guide les actions et les initiatives de l'UE en matière de cybersécurité pour la décennie à venir. Elle devrait être révisée dans le cadre de la prochaine législature.

Possibles conséquences pour la Suisse

La stratégie n'est pas destinée à la Suisse mais pourrait avoir des conséquences indirectes :

- **Harmonisation des normes et réglementations** : Pour faciliter la coopération et le commerce avec les Etats membres de l'UE, la Suisse pourrait être amenée à aligner ses propres normes et réglementations de cybersécurité sur celles promues par l'UE, en adoptant par exemple de nouvelles technologies de sécurité, de meilleures pratiques et des cadres de conformité similaires à ceux de l'UE.
- **Renforcement de la coopération** : La stratégie encourage une coopération internationale accrue en matière de cybersécurité. La Suisse étant un partenaire clé pour les Etats membres de l'UE, elle pourrait intensifier sa collaboration avec les institutions européennes de cybersécurité, participer à des exercices conjoints de réponse aux incidents et partager des informations sur les menaces et les vulnérabilités.
- **Conséquences pour les entreprises suisses** : Les nouvelles normes de cybersécurité de l'UE pourraient avoir des conséquences notamment sur les entreprises suisses qui opèrent au niveau

international ou qui ont des partenariats avec des entités de l'UE. En effet, il se peut qu'elles doivent améliorer leurs mesures de sécurité pour rester compétitives et conformes aux attentes de leurs partenaires.

- **Participation à des initiatives européennes**: La Suisse pourrait participer à certaines initiatives européennes de cybersécurité, telles que les programmes de recherche et de développement en cybersécurité, les réseaux de coopération en matière de crise cybernétique et d'autres projets visant à renforcer la résilience cybernétique. Elle pourrait notamment le faire au travers du programme de recherche Horizon Europe, pour lequel un accord d'association est actuellement en cours de négociation.

Mesures déjà prises en Suisse

La Suisse n'a pas pris de mesures spéciales pour s'harmoniser avec la stratégie, mais la révision de la loi sur la sécurité de l'information (LSI) et la Cyberstratégie Nationale (CSN) vont, pour beaucoup, dans le même sens.

Mesure 16

Cyber Resilience Act

Appellation complète de la mesure	Règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques
Type de mesure	Règlement
Référence	Règlement (EU) 2024/2847
Etat actuel	Entrée en vigueur
Date d'entrée en vigueur	10.12.2024
Unité responsable dans l'administration fédérale	OFCS/OFCOM

Description

Le 15 septembre 2022, la Commission européenne (COM) a présenté une proposition de règlement sur les exigences horizontales de cybersécurité applicables aux produits contenant des éléments numériques (Cyber Resilience Act, CRA). Cet acte législatif, qui complète la directive NIS-2, s'appuie sur la stratégie de cybersécurité 2020 de l'UE et sur la stratégie 2020 de l'UE en matière de sécurité. Le Parlement européen et le Conseil de l'UE sont parvenus à un accord provisoire sur le texte du règlement en novembre 2023.

Le CRA constitue la première législation européenne commune visant à garantir la cybersécurité de tous les produits connectés directement ou indirectement à un autre appareil ou à un réseau via une connexion de données logique ou physique. Quelques exceptions sont prévues pour les produits déjà soumis à des exigences de cybersécurité inscrites dans la législation européenne en vigueur, par exemple les dispositifs médicaux, les produits aéronautiques ou les véhicules à moteur.

Le règlement distingue produits critiques et produits non critiques. Ces derniers représentent 90% des produits du marché. Il s'agit surtout de produits de consommation privée, dont la cybersécurité doit être évaluée par les fabricants eux-mêmes. Les **produits critiques** désignent les infrastructures centrales de l'Etat et, entre autres, les VPN, les pare-feux ou les systèmes d'exploitation. Ils se répartissent en classe I et II. Les produits critiques de classe II doivent faire l'objet d'une évaluation de conformité indépendante confiée à un tiers. Quant aux produits critiques de classe I, ilssont eux aussi soumis à une évaluation indépendante confiée à un tiers, à moins que des normes harmonisées ne soient appliquées. L'acte législatif vise à garantir la "cybersécurité dès la conception", à savoir que la création de produits doit dès le départ avoir pour objectif qu'ils soient cybersécurisés.

En outre, les nouvelles règles **transfèrent la responsabilité aux fabricants**. Ceux-ci devront garantir que les produits mis sur le marché de l'UE et qui contiennent des éléments numériques sont conformes aux exigences de sécurité pendant leur durée de vie ou pendant cinq ans, à l'exception des produits dont l'utilisation prévue est plus courte.

Enfin, les fabricants doivent **signaler dans les 24 heures** à l'équipe nationale de réponse aux incidents de sécurité informatique (Computer Security Incident Response Team - CSIRT, ancrée dans NIS-2) ainsi qu'à l'Agence de cybersécurité de l'UE (ENISA) toute vulnérabilité d'un produit activement exploitée ou tout incident ayant de graves répercussions sur la sécurité. Dans certaines circonstances, la CSIRT peut, à des fins de cybersécurité, décider de limiter les informations transmises à l'ENISA.

Situation actuelle

Le 12 mars 2024, le Parlement européen a adopté l'accord politique sur le Cyber Resilience Act conclu avec le Conseil de l'UE en novembre 2023. Le 17 mars 2024, la Commission a publié un projet de mandat de normalisation pour le CENELEC afin que les normes harmonisées nécessaires au CRA soient développées. Le 10 octobre 2024, le texte du règlement a été adopté par le Conseil de l'UE. Le texte final a été publié au Journal officiel de l'UE le 20 novembre 2024 et est entré en vigueur le 10 décembre 2024. Par conséquent, la mise en œuvre du CRA se fera en plusieurs étapes de fin 2024 à 2027 :

- 11 avril 2026 : Les organismes d'évaluation de la conformité (OEC) sont habilités à évaluer la conformité des produits aux exigences du CRA.
- 11 septembre 2026 : Les fabricants de produits connectés sont soumis à une obligation de notification des vulnérabilités et des incidents.
- 11 décembre 2027 : Toutes les exigences du CRA s'appliquent, y compris la conformité aux exigences de base en matière de cybersécurité avant la mise sur le marché d'un produit, le traitement des vulnérabilités tout au long du cycle de vie du produit et la transparence vis-à-vis des utilisateurs.

Possibles conséquences pour la Suisse

Le Cyber Resilience Act de l'UE affecte la Suisse de plusieurs manières :

- **Harmonisation des normes** : La Suisse, concrètement les entreprises qui échangent avec l'UE, risque de se heurter à des obstacles commerciaux. Elle pourrait décider d'adopter des normes de sécurité similaires pour garantir la compatibilité avec l'UE et réduire ainsi ces obstacles.
- **Conséquences indirectes** : Même si la Suisse n'adopte pas directement les nouvelles réglementations de l'UE, les entreprises et les autorités pourraient tirer bénéfice du renforcement des exigences de sécurité, lequel améliorerait globalement la cybersécurité en Europe, notamment en ce qui concerne les produits conformes à l'UE proposés par des entreprises étrangères en Suisse.
- **Mise à l'écart de l'échange d'informations opérationnelles au niveau de l'UE :** La Suisse ne fait pas partie des réseaux de CSIRT, ce qui peut s'avérer désavantageux pour elle si le réseau contribue à une approche coordonnée ou si des actions communes coordonnées sont menées (comme avec l'EU Product Compliance Network - EUPCN).
- **Conséquences pour l'économie :** Les entreprises suisses qui exportent vers l'UE doivent respecter les obligations susmentionnées (obligations d'évaluer et de consigner les cyberrisques, de signaler les vulnérabilités exploitées activement, ainsi que de surveiller les mises à jour de sécurité et les vulnérabilités, et d'éliminer ces dernières pendant la durée de vie prévue du produit). Les fabricants doivent démontrer qu'ils ont respecté les exigences en matière de cybersécurité. Selon la classification des risques du produit concerné, ils le font par le biais d'une autodéclaration ou d'une évaluation confiée à des organismes d'évaluation de la conformité dans l'UE, comme le requiert la législation européenne (produits importants et critiques contenant des éléments numériques). Les importateurs européens de produits suisses contenant des éléments numériques doivent en outre indiquer leurs nom, adresse, coordonnées numériques et, le cas échéant, leur site web, soit sur le produit, soit sur son emballage, soit dans les documents qui l'accompagnent.

La Suisse a conclu un accord avec l'UE sur la reconnaissance mutuelle en matière d'évaluation de la conformité pour des produits de 20 secteurs. Cet accord aura des conséquences pour les secteurs concernés (en particulier les machines) car ses exigences s'ajouteront à celles qui existent déjà pour l'accès au marché. Il convient d'examiner s'il pourrait être étendu afin d'inclure les exigences en matière de cybersécurité et de réduire ainsi les éventuelles entraves au commerce. On ne sait toujours pas quand l'UE sera à nouveau prête à mettre à jour l'ARM dans le contexte des relations entre la Suisse et l'UE.

Mesures déjà prises en Suisse

La Suisse a déjà pris les mesures suivantes de sa propre initiative :

- Cyberstratégie Nationale CSN ;
- Mise en place et renforcement de l'OFCS, par exemple avec l'instauration d'une gestion stratégique des vulnérabilités et l'établissement de processus RVD dans ce contexte.
- Intensification de la coopération internationale en matière de cybersécurité dans le cadre d'une coopération bilatérale et régionale sur la normalisation et le développement technologique.
- Reprise du "règlement délégué (UE) 2022/30 de la COM complétant la directive 2014/53/UE introduisant des exigences de cybersécurité pour certains types d'équipements de radiocommunication" dans l'ordonnance sur les installations de radiocommunication (OIT) ainsi que dans l'ordonnance de l'OFCOM sur les installations de radiocommunication (OOIT). Les exigences s'appliqueront à partir du 1er août 2025. Elles seront concrétisées dans un paquet de trois normes harmonisées actuellement développées par le CENELEC (Comité européen de normalisation en électronique et en électrotechnique) (FprEN 18031-1, FprEN 18031-2 et FprEN 18031-3). En Suisse, c'est l'OFCOM qui est chargé de l'exécution.
- Législation d'application de l'art. 48a LTC: conformément à l'art. 96a, al. 3, OST, les fournisseurs d'accès à internet doivent entretenir et mettre à jour les modems qu'ils fournissent.

Mesure 17

Directive SRI 2

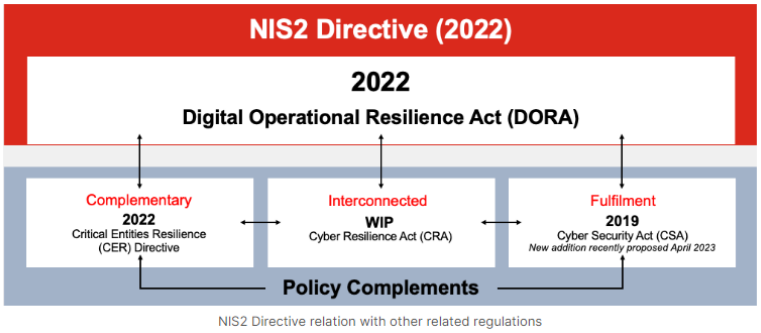
Appellation complète de la mesure	Directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union
Type de mesure	Directive
Référence	Directive (UE 2022/2555)
Etat actuel	En vigueur
Date d'entrée en vigueur	16.01.2023
Unité responsable dans l'administration fédérale	OFCS/OFCOM

Description

La révision de la directive (UE 2022/2555) concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI-2) a pour objectif d'améliorer encore les capacités de réaction des secteurs public et privé aux incidents de sécurité. Elle élargit tout d'abord le champ d'application des dispositions. Jusqu'à présent, la directive prévoyait que les Etats membres de l'UE définissent selon certains critères les entités considérées comme des opérateurs de services essentiels. Désormais, elle s'applique à toutes les moyennes et grandes entités (au-delà d'un certain seuil) actives dans les secteurs concernés ou fournissant des services correspondants. Elle couvre également les moyennes et grandes entités d'un plus grand nombre de secteurs essentiels à l'économie et à la société, notamment les fournisseurs de services de communication électroniques et de services numériques, le secteur des eaux usées et les services postaux au niveau central et régional. Elle s'applique également aux administrations publiques au niveau central et régional, mais pas aux entités de secteurs tels que la défense, la sécurité nationale et publique, la justice, les banques ou les parlements. Toutefois, les Etats membres de l'UE peuvent décider qu'elle s'applique également au niveau local.

Les entités relevant du champ d'application de la directive doivent **notifier les cyberincidents sous 24 heures** et fournir, dans les trois jours au plus tard, un rapport détaillé comprenant une première évaluation de l'incident de sécurité, de sa gravité et de ses conséquences, ainsi que tout indicateur de compromission (IoC). La directive introduit également un nouveau système de recours et de sanctions.

Les entités qui ne respectent pas la législation s'exposent à des amendes pouvant aller jusqu'à 2% de leur chiffre d'affaires. La directive officialise par ailleurs la création des réseaux européens CSIRT et EU-CyCLONe en tant qu'organisations de liaison pour les cybercrises, chargées de soutenir la coopération et la gestion coordonnée des incidents majeurs. La coopération au sein des réseaux est encouragée par des appels d'offres lancés dans le cadre du programme Digital Europe (volet cybersécurité). Un mécanisme volontaire d'apprentissage par les pairs est également mis en place afin de renforcer la confiance mutuelle et d'améliorer l'apprentissage sur la base des bonnes pratiques et des expériences. La directive sert également de modèle de référence pour la coopération de l'UE avec les pays tiers, via la fourniture d'une assistance technique externe, et renforce le rôle du groupe de coopération (représentants des Etats membres de l'UE, de la Commission et de l'ENISA) dans les décisions politiques stratégiques. Les interdépendances entre les différentes directives et législations de l'UE relatives à la directive SRI 2 se présentent comme suit :



NIS2 Directive relation with other related regulations

Situation actuelle

La directive est entrée en vigueur le 16 janvier 2023. Les Etats membres de l'UE ont 21 mois à compter de cette date pour en transposer les dispositions dans leur droit national, à savoir adapter leurs lois et réglementations internes pour se conformer aux nouvelles exigences.

Les principaux éléments qui doivent être mis en œuvre sont les suivants :

- **Etablissement des seuils :** Les Etats membres de l'UE doivent définir des seuils spécifiques pour déterminer quelles entités moyennes et grandes sont soumises aux obligations de la directive SRI 2.
- **Mise en place des mesures de signalement** : Les entités couvertes par la directive doivent mettre en place des mécanismes permettant de signaler les incidents de cybersécurité dans les 24 heures et de présenter des rapports détaillés dans les trois jours suivant un incident.
- **Système de sanctions et de recours** : Les Etats membres de l'UE doivent établir des systèmes de sanctions à l'encontre des entités qui ne respectent pas les exigences de la directive ainsi que des mécanismes de recours permettant aux entités concernées de contester ces sanctions.
- **Développement de capacités :** Les secteurs public et privé doivent renforcer leurs capacités de cybersécurité pour répondre aux exigences accrues de la directive, par exemple en formant du personnel, en améliorant les infrastructures de sécurité ou en recourant à de nouvelles technologies de cybersécurité.
- **Création de structures de coopération** : La directive prévoit la création des Réseaux européens des organisations de liaison pour les crises cybernétiques (EU-CyCLONe, CSIRT). Les Etats membres de l'UE doivent donc participer à la mise en place et au fonctionnement de ces réseaux pour assurer une coopération efficace en cas d'incidents majeurs.
- **Rapports et évaluations** : Les Etats membres de l'UE doivent rendre compte régulièrement à la Commission de la mise en œuvre de la directive et de l'état de la cybersécurité. Ils doivent notamment mener des évaluations périodiques pour identifier les domaines nécessitant des améliorations ou des ajustements.
- **Assistance technique et coopération internationale** : La directive prévoit également un modèle de référence pour la coopération avec des pays tiers. Les Etats membres de l'UE doivent donc travailler à établir et à renforcer ces partenariats internationaux en matière de cybersécurité.

Possibles conséquences pour la Suisse

La directive SRI 2 pourrait avoir plusieurs conséquences indirectes sur la Suisse, notamment en raison de la forte interconnexion entre les infrastructures et les entreprises suisses et européennes. Pour maintenir leurs relations commerciales, les entreprises suisses opérant dans des secteurs critiques et ayant des interactions avec l'UE, ou fournissant des services à des clients basés dans l'UE, pourraient devoir se conformer aux exigences de la directive SRI 2, par exemple en mettant en place des mesures de cybersécurité adéquates et en améliorant les possibilités de signaler les incidents de sécurité.

Mesures déjà prises en Suisse

La loi sur la sécurité de l'information (LSI) prévoit notamment une obligation de signaler les cyberincidents qui concernent les infrastructures critiques. Cette obligation de notification représente une certaine compatibilité avec l'obligation de notification introduite dans l'UE après la SRI 1.

Mesure 18

Directive CER

Appellation complète de la mesure	Révision de la directive sur la résilience des entités critiques (CER)
Type de mesure	Directive
Référence	Directive (UE) 2022/2557
Etat actuel	En vigueur
Date d'entrée en vigueur	16.01.2023
Unité responsable dans l'administration fédérale	OFCS/OFCOM/DFAE-Digi

Description

La directive sur la résilience des entités critiques (Critical Entities Resilience, CER) est entrée en vigueur le 16 janvier 2023. Elle remplace et élargit en substance le champ d'application de la directive de 2008 sur les infrastructures critiques européennes, qui ne s'appliquait qu'aux secteurs de l'énergie et des transports. La nouvelle directive couvre onze secteurs (**énergie, transports, banques, infrastructure des marchés financiers, santé, eau potable, eaux usées, infrastructure numérique, administration publique, espace et production, transformation et distribution de denrées alimentaires).** Elle établit un cadre destiné à aider les Etats membres de l'UE à réduire la vulnérabilité des installations critiques et à en renforcer la résilience physique. Elle prévoit que les Etats membres élaborent une stratégie nationale de renforcement de la résilience des installations critiques, procèdent à une évaluation des risques au moins tous les quatre ans et dressent une **liste des installations critiques** fournissant des services essentiels. Les exploitants de ces installations doivent identifier les risques susceptibles de perturber de manière significative la fourniture de services essentiels, prendre des mesures pour en assurer la résilience et notifier les incidents aux autorités compétentes. Les appels d'offres du programme Horizon Europe (Cluster 3, Infrastructures résilientes) encouragent la coopération pour la mise en œuvre de la directive. La directive contient en outre des dispositions spécifiques aux installations critiques d'"importance européenne particulière", à savoir celles qui fournissent un service essentiel à six Etats membres ou plus.

Situation actuelle

Le 25 juillet 2023, dans le cadre d'un acte délégué, la Commission a adopté une liste de services essentiels pour les onze secteurs énumérés dans la directive REC. Les Etats membres doivent recenser les installations critiques concernées d'ici au 17 juillet 2026. Ils se réfèrent à la liste des services essentiels pour évaluer les risques et identifier les installations critiques.

Possibles conséquences pour la Suisse

La directive n'a pas de conséquences directes pour la Suisse. Il peut être important que les fournisseurs d'infrastructures critiques sachent quels secteurs sont considérés comme critiques dans l'UE.

Mesures déjà prises en Suisse

La Suisse a déjà identifié ses secteurs et sous-secteurs critiques dans la "Stratégie nationale de protection des infrastructures critiques".

Mesure 19

Cyber Solidarity Act

Appellation complète de la mesure	Règlement établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir
Type de mesure	Règlement
Référence	Règlement (UE) 2025/38
Etat actuel	En vigueur
Date d'entrée en vigueur	04.02.2025
Unité responsable dans l'administration fédérale	OFCS

Description

Le règlement établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir (Cyber Solidarity Act, CSA) est entré en vigueur le 4 février 2025. Le texte a pour but de renforcer les capacités communes de l'UE à détecter les menaces et incidents de cybersécurité importants, à s'y préparer et à y réagir.

Les principaux points du CSA sont les suivants :

- Création d'un **système d'alerte européen en matière de cybersécurité**, composé de *cyberhubs* nationaux et transfrontaliers. Outre l'échange d'informations, les *cyberhubs* sont chargés de détecter et d'analyser les cybermenaces. Les Etats membres participent à ce système sur une base volontaire.
- Création d'un **mécanisme de cyberurgence** destiné à apporter un soutien financier et organisationnel aux Etats membres de l'UE pour les tests sur les vulnérabilités potentielles des installations critiques (p. ex. dans les secteurs de la santé, des transports et de l'énergie) et pour l'encouragement à l'assistance mutuelle entre les autorités nationales.
- Création d'une **réserve de cybersécurité de l'UE**, composée de services d'urgence pour les incidents de sécurité du secteur privé. Elle peut intervenir en cas d'incident de cybersécurité majeur, à la demande d'un Etat membre de l'UE ou d'autres entités de l'UE. En outre, les pays tiers associés à Digital Europe peuvent également solliciter cette aide, à condition que leur participation à la réserve soit prévue dans l'accord d'association.
- Création d'un mécanisme d'**enquête sur les incidents graves de cybersécurité** par l'Agence de l'UE pour la cybersécurité (ENISA).

Situation actuelle

Le Cyber Solidarity Act a été publié dans le Journal Officiel de l'UE le 15 janvier 2025 et est entré en vigueur le 4 février 2025.

Possibles conséquences pour la Suisse

La Suisse n'est concernée qu'indirectement par les mesures de l'UE. Elle pratique un échange d'informations étroit avec différentes autorités nationales d'Etats membres de l'UE. Cet échange est important pour la détection précoce. Il n'y a pas de raison que le Cyber Solidarity Act complique cet échange, et la Suisse devrait continuer à obtenir les informations nécessaires par le biais de contacts directs entre spécialistes.

Un accès à la réserve de cybersécurité de l'UE ne constitue pas une mesure urgente pour la Suisse, où les autorités et le secteur privé collaborent déjà étroitement.

Mesures déjà prises en Suisse

Un service d'enquête sur les incidents de cybersécurité est créé à l'Office fédéral de la cybersécurité. Ces deux initiatives ont été lancées sur une initiative propre. L'échange avec les Etats membres de l'UE est assuré.

Mesure 20

Règlement sur l’éconception

Appellation complète de la mesure	Règlement établissant un cadre pour la fixation d’exigences en matière d’écoconception pour des produits durables
Type de mesure	Règlement
Référence	Règlement (UE) 2024/1781
Etat actuel	En vigueur
Date d’entrée en vigueur	18.07.2024
Unité responsable dans l’administration fédérale	BAFU

Description

Le règlement sur l'écoconception (Ecodesign Regulation, ESPR) établit un cadre général et harmonisé pour la définition d'exigences en matière de conception des produits. Il remplace l'actuelle directive 2009/125/CE sur l'écoconception et en élargit le champ d'application. Au-delà des produits énergétiques, le nouvel acte législatif s'applique désormais à tous les types de biens mis sur le marché de l'UE.

Le règlement concerne presque tous les types de produits, à quelques exceptions près, comme les médicaments, les véhicules, les denrées alimentaires et les aliments pour animaux, ainsi que les produits liés à la sécurité et à la défense. Le ESPR établit un cadre juridique pour l'introduction de nouvelles exigences dans les domaines suivants : la durabilité, la réutilisation, l’amélioration et la réparabilité des produits, la présence de substances qui empêchent le recyclage, l’efficacité énergétique et l’efficacité des ressources, la part de matières recyclées, la remise à neuf et le recyclage, l’empreinte des gaz à effet de serre et l’empreinte environnementale, ainsi que les exigences en matière d’informations, dont un passeport numérique des produits (DPP). La Commission européenne est habilitée à adopter des actes délégués fixant des exigences d'écoconception, auxquelles l'industrie doit en principe se conformer dans un délai de 18 mois. Enfin, les marchés en ligne ont l’obligation de coopérer avec les autorités de surveillance du marché.

Le passeport numérique des produits contient un ensemble de données spécifiques à un produit, à savoir les informations mentionnées dans les actes délégués applicables. Il est accessible via un support électronique (p. ex. un code QR). Il permet à l'UE de non seulement mettre à disposition numériquement les informations d'écoconception, mais aussi les preuves de conformité, la documentation technique ainsi que d'autres informations liées au produit (p. ex. manuels d'utilisation, instructions d'emploi, informations de sécurité). Ces informations doivent être recueillies et stockées de manière décentralisée tout au long de la chaîne de valeur industrielle et être rendues accessibles de différentes manières aux consommateurs, aux acteurs économiques et aux. Il incombe aux importateurs de veiller à ce que les produits en provenance de pays tiers soient conformes aux exigences d'écoconception et accompagnés d'un passeport numérique des produits. L'UE disposera d’un registre DPP central, qui regroupera tous les identifiants uniques des produits commercialisés ou mis en service dans l'UE (UID) et auquel les autorités des Etats membres de l'UE chargées de la surveillance du marché auront accès. La Commission créera un portail web qui permettra aux consommateurs de rechercher et de comparer une partie des données contenues dans le passeport.

Les marchés publics sont désormais soumis à des critères d'écoconception afin d'inciter à l'achat de produits respectueux de l'environnement. Le nouveau règlement introduit une interdiction directe de détruire les textiles et les chaussures invendus (les PME en sont temporairement exemptées), qui pourrait s’appliquer à d’autre produits si la Commission fait usage de son pouvoir d'adopter des interdictions similaires. S’agissant des produits vendus en ligne, le règlement sur l'écoconception correspond à la loi sur les services numériques.

Le règlement sur l'écoconception présente un lien au niveau du contenu avec d'autres projets législatifs de l'UE, notamment avec les directives européennes sur 1) la promotion de la réparation des biens (droit à la réparation), 2) le renforcement du rôle des consommateurs, 3) la responsabilité du fait des produits défectueux, 4) les droits des consommateurs, 5) les allégations environnementales (*green claims*) et 6) les pratiques commerciales déloyales.

Situation actuelle

Le règlement est entré en vigueur le 18 juillet 2024. Après une période de transition de 24 mois, il interdira la destruction des textiles et des chaussures invendus. Il confère en outre à la Commission le pouvoir d'adopter des actes délégués établissant des exigences d'écoconception. Les premiers actes délégués pourraient être adoptés fin 2025, avec une période transitoire de 18 mois. Le premier passeport numérique sera introduit en 2027 avec le règlement relatif aux batteries (UE) 2023/1542 pour les batteries de véhicules électriques, les batteries pour les transports légers et les grandes batteries industrielles (> 2kWh). Le règlement sur les produits de construction (en passe d'être formellement adopté) et la proposition de règlement sur les jouets prévoient un passeport pour 2028.

Possibles conséquences pour la Suisse

Les effets concrets dépendent notamment des actes délégués relatifs aux différents produits qui entreront en vigueur dans les prochaines années.

Une analyse d'impact réalisée en 2022 a montré qu'une reprise par la Suisse des exigences d'écoconception examinées permettrait d'obtenir un rapport coûts/bénéfices positif. La plupart des exigences édictées dans le cadre de la directive européenne sur l'écoconception (actuellement encore en vigueur), qui concernaient principalement des aspects liés à l'énergie, ont été reprises dans l'ordonnance suisse sur les exigences relatives à l'efficacité énergétique (OEEE). Cet alignement sur les règles, catégories et termes utilisés dans l'UE répond à la loi fédérale sur les entraves techniques au commerce (LETC). Pour les fabricants, importateurs et distributeurs suisses concernés, il facilite les échanges de marchandises avec l'UE.

En raison des nouvelles exigences de l'ESPR, les fabricants suisses qui commercialisent leurs produits dans l'UE devraient faire examiner leurs produits relevant des domaines où l'évaluation de la conformité est effectuée par des organismes tiers par des organismes dans l'UE. En outre, dans certains domaines (p. ex. construction), les exportateurs devraient désigner un mandataire ayant son siège dans l'UE. Les fabricants et les importateurs devraient quant à eux indiquer leur adresse à la fois sur le produit lui-même et dans son passeport numérique. A l'inverse, compte tenu des liens économiques étroits, des produits munis d'un passeport dans l'UE sont susceptibles d'apparaître également sur le marché suisse. La Suisse devrait donc s'assurer que dans ces cas, elle continue à avoir accès aux informations destinées aux consommateurs, mais aussi aux autorités d'exécution et aux organes douaniers.

Les fabricants suisses qui mettent des produits à disposition sur le marché de l'UE pourront probablement en établir eux-mêmes le passeport, recueillir et stocker des informations, s'enregistrer dans le registre et conserver une copie de sauvegarde auprès d'un prestataire de services correspondants. Les acteurs économiques qui fournissent des produits à la fois sur le marché de l'UE et sur le marché suisse verraient probablement leur charge administrative réduite si la Suisse pouvait participer au système DPP de l'UE ou introduire un système DPP interopérable identique et ancrer contractuellement son équivalence avec l'UE. En outre, puisque dans l'UE les preuves de conformité et les documents techniques seront eux aussi mis à disposition sous forme numérique via le passeport, la surveillance du marché s'en trouvera facilitée, notamment si l'accès aux informations protégées pouvait être convenu par contrat avec l'UE.

La Suisse a aujourd'hui un accord avec l'UE sur la reconnaissance mutuelle en matière d'évaluation de la conformité (ARM) pour des produits dans 20 secteurs. Il semble que l'UE introduira également des exigences d'écoconception, y compris des DPP, pour des secteurs de produits tels que les produits de construction et les jouets, qui sont couverts par l'ARM. Dans ces secteurs de produits, les réglementations techniques de la Suisse et de l'UE sont reconnues comme équivalentes dans le cadre de l'ARM. La question de savoir si l'accord ARM pourrait être étendu afin d'inclure les exigences d'écoconception et de réduire ainsi les éventuelles entraves au commerce doit être examinée. Il n'est toujours pas clair à partir de quand l'UE sera à nouveau prête à mettre à jour l'ARM dans le contexte des relations entre la Suisse et l'UE.

Mesures déjà prises en Suisse

Pratique actuelle : Depuis plusieurs années, la Suisse reprend dans l'ordonnance sur les exigences relatives à l'efficacité énergétique (OEEE) la plupart des exigences relatives à ce sujet inscrites dans les ordonnances d'application de la directive sur l'écoconception. En 2020, pour six groupes de produits (p. ex. les lave-linges et les lave-vaisselle), des exigences relatives à l'efficacité des ressources, notamment à la disponibilité des pièces de rechange et d'instructions de réparation, ont été intégrées pour la première fois.

Nouvelle base légale : Le 15 mars 2024, l'initiative parlementaire 20.433 Développer l'économie circulaire en Suisse a été adoptée par le Parlement. Après l'expiration du délai référendaire le 4 juillet, le Conseil fédéral a décidé de son entrée en vigueur. L'art. 35i LPE habilite le Conseil fédéral à imposer sur les produits des exigences d'écoconception et de créer ainsi des conditions d'accès au marché identiques pour les entreprises situées en Suisse ou dans l'UE. Il mentionne explicitement que le Conseil fédéral doit tenir compte des dispositions des principaux partenaires commerciaux.

Passeports numériques pour les produits : L'art. 35i concerne également les exigences relatives à l'étiquetage des produits et à la mise à disposition d'informations. Si l'introduction du passeport devenait possible, il conviendrait d'examiner une nouvelle adaptation des bases légales. De leur propre initiative, les offices fédéraux concernés ont commencé à examiner les options d'action.

Marchés publics : L'initiative parlementaire prévoit que l'art. 30, al. 4, LMP renforce les marchés publics durables.

Interdire et signaler la destruction des textiles et des chaussures : D'un point de vue économique et écologique, il convient d'éviter dans la mesure du possible de détruire des produits neufs invendus. Le Conseil fédéral le dit aussi, dans sa réponse du 23.08.2023 à l'intervention: 23.3649 | Ne jetons plus les produis non alimentaires invendus! | Objet | Le Parlement suisse. Il peut, sur la base de l'art. 46, al. 2, de la loi sur la protection de l'environnement (LPE, RS 814.01), obliger, par voie d'ordonnance, les entreprises à collecter des données sur les déchets et leur élimination, et à mettre sur demande ces données à disposition de la Confédération. Jusqu'à présent, il n'a pas jugé nécessaire d'agir à ce sujet. A ce jour, il n'existe pas en Suisse d'interdiction de détruire les invendus neufs.

Mesure 21

Plan d’action en matière d’éducation numérique

Appellation complète de la mesure	Plan d’action en matière d’éducation numérique
Type de mesure	Plan d’action
Référence	Plan d'action en matière d'éducation numérique (2021-2027)
Etat actuel	En vigueur
Date d’entrée en vigueur	30.09.2022
Unité responsable dans l’administration fédérale	SEFRI

Description

Le Plan d'action en matière d'éducation numérique (2021-2027) prévoit d'adapter l'éducation et la formation à l'ère numérique et de tirer les leçons de la crise du covid-19, notamment en matière d'utilisation des technologies numériques dans le domaine de l'éducation. Le plan d'action prévoit deux priorités centrales :

La promotion d'un écosystème d'éducation numérique performant (priorité stratégique 1) dans les domaines des infrastructures, de la formation des enseignants, des contenus d'enseignement et des outils ainsi **que le déploiement des compétences numériques** (priorité stratégique 2), qu'il s'agisse des compétences de base des plus jeunes ou de la formation d'un plus grand nombre de spécialistes en informatique, en mettant l'accent sur la promotion des filles et des femmes. Pour réaliser ces priorités, la Commission européenne (COM) souhaite promouvoir les échanges entre les Etats membres de l'UE, élaborer des lignes directrices et des études de faisabilité dans différents domaines, développer des nouveaux outils (p. ex. l'outil d'autoévaluation SELFIE pour les enseignants, lancé en octobre 2021) et mettre à profit des synergies avec les programmes Erasmus+, Horizon Europe ou Europe numérique.

Le **Pôle européen d'éducation numérique** (European Digital Education Hub) est l'une des actions phares du Plan d'action en matière d’éducation numérique. Cette communauté virtuelle et collaborative a pour objectif de renforcer la coopération, la collaboration et les synergies intersectorielles pour l'éducation numérique en Europe. Elle relie les acteurs de l'ensemble de l'écosystème de l'éducation numérique (formelle, non formelle et informelle) et il soutient les activités destinées à aborder les questions clés qui concernent la politique et la pratique. Le pôle soutiendra le monitorage de l'éducation numérique en Europe et la mise en œuvre du plan d'action en matière d’éducation numérique. Il offre des ateliers destinés à la communauté, un échange virtuel d’expériences, du mentoring et un accélérateur de projets.

Situation actuelle

Le plan d’action est en cours de mise en œuvre, durée : de 2021 à 2027.

Mesures réalisées, exemples :

- Recommandation du Conseil relative aux principaux facteurs favorisant la réussite de l’éducation et de la formation numériques
- Recommandation du Conseil sur des approches d’apprentissage hybride pour une éducation primaire et secondaire inclusive et de haute qualité
- Lignes directrices éthiques sur l’utilisation de l’intelligence artificielle (IA) et des données dans l’enseignement et l’apprentissage à l’intention des éducateurs

Prochaines étapes, exemples :

- Soutien au développement de plans de transformation numérique pour les établissements d’enseignement et de formation, au moyen de projets de coopération Erasmus+ (en cours)
- Développement d’un cadre européen pour les contenus éducatifs numériques

- Création d'une plateforme européenne d'échange de données éducatives et de contenus de l'enseignement supérieur

Comme il s'agit d'un plan d'action et non pas d'une règlementation au niveau juridique, les mesures adoptées par la COM n'entrent pas en vigueur à proprement parler, et les Etats membres n'ont pas d'obligation à les mettre en œuvre. Les mesures principales se traduisent en recommandations du Conseil, en cadres de référence ou encore en lignes directrices pour l'éducation numérique. Les mesures sont développées et adoptées au fur et à mesure pendant la durée du plan d'action.

Possibles conséquences pour la Suisse

Aucun accord bilatéral n'ayant été conclu dans ce domaine, les propositions de la COM n'ont pas d'effet contraignant sur la Suisse. Cependant, du moment que celle-ci partage avec l'UE des priorités similaires, il est important qu'elle suive attentivement les travaux de l'UE dans le domaine de la numérisation de l'éducation. Jusqu'à la fin de l'année 2021, la Suisse a participé régulièrement aux réunions d'experts du ET2020 Working Group "Digital Education : Learning, Teaching and Assessment (WG DELTA)" de la COM. Le groupe est consulté régulièrement dans le cadre de la mise en œuvre du Plan d'action en matière d'éducation numérique. Depuis 2022, l'UE en a toutefois exclu la Suisse pour des raisons politiques. Bien que la responsabilité du contenu de l'enseignement incombe en premier lieu aux cantons, la Suisse tirerait profit du partage et de l'échange de bonnes pratiques en matière d'éducation numérique au sein de l'UE et pourrait s'inspirer des outils (p. ex. SELFIE) et des cadres communs (p. ex. DigCompEdu) européens.
S'agissant du Pôle européen d'éducation numérique, l'inscription au pôle et à sa communauté virtuelle est gratuite et ouverte à tout le monde. Les acteurs suisses peuvent donc participer aux discussions et aux échanges de bonnes pratiques, mais certaines activités sont réservées exclusivement aux Etats membres.

Mesures déjà prises en Suisse

Les priorités stratégiques du plan d'action en matière d'éducation numérique représentent aussi des priorités de la politique suisse concernant l'espace de formation.
Quant à la priorité stratégique 1, la Suisse poursuit également l'objectif d'articuler des politiques pertinentes pour l'éducation numérique et de créer un écosystème dans ce domaine. Ainsi, afin d'assurer la cohérence entre les initiatives fédérales et cantonales, la Confédération et les cantons collaborent étroitement, dans les limites de leurs compétences respectives, au sein du comité de coordination "Numérisation de l'éducation".
Quant à la priorité stratégique 2, la Confédération prend également des mesures ciblées, en collaboration avec les cantons et les autres acteurs du domaine de la Formation, de la Recherche et de l'Innovation (FRI), pour soutenir le développement des compétences numériques. Le plan d'action "Numérisation pour le domaine FRI durant les années 2019 et 2020" - élaboré par le Secrétariat d'Etat à la formation, à la recherche et à l'innovation (SEFRI), en étroite collaboration avec les acteurs du monde de la formation et de la recherche - ainsi que le traitement de la numérisation comme thème transversal dans les messages d'encouragement FRI 2021 à 2024 et 2025 à 2028 traduisent cette volonté. Une vue d'ensemble des mesures prises pour la période d'encouragement FRI 2025 à 2028 en matière de numérisation et en particulier de compétences numériques est disponible sur le site du SEFRI.

Mesure 22

Directive relative au travail via une plateforme

Appellation complète de la mesure	Directive relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme
Type de mesure	Directive
Référence	Directive (UE) 2024/2831
Etat actuel	En vigueur
Date d'entrée en vigueur	01.12.2024
Unité responsable dans l'administration fédérale	OFAS

Description

Le 9 décembre 2021, la Commission européenne a présenté un ensemble de mesures visant à réglementer et améliorer globalement les conditions de travail des travailleurs des plateformes numériques. Les propositions ont pour objectif que les travailleurs puissent bénéficier des droits et des prestations sociales auxquels ils peuvent légitimement prétendre. La proposition se compose d'une communication, d'une proposition de directive, ainsi que d'un projet de lignes directrices.

Dans sa communication, la Commission a fourni des informations sur l'approche et les mesures à adopter en matière de travail via une plateforme. Les mesures sont en outre complétées par des actions que les autorités nationales, les partenaires sociaux et les autres acteurs pertinents devraient mettre en œuvre à leur niveau respectif. Il s'agit également de poser les bases en vue de l'élaboration de futures normes mondiales garantissant la qualité du travail via une plateforme.

La proposition de directive relative à l'amélioration des conditions de travail vise d'abord à garantir que les personnes qui exécutent un travail via une plateforme obtiennent le statut juridique professionnel qui correspond à leurs modalités réelles de travail (lutte contre le "faux travail indépendant"). Elle prévoit à cet effet une présomption en faveur de la qualité de travailleur pour les personnes qui travaillent via des plateformes. Contrairement à la proposition initiale de la Commission et à la position de négociation du Parlement européen, elle ne contient plus de liste de critères pour déterminer l'existence d'une relation de travail. Le texte juridique adopté prévoit plutôt l'activation de la présomption de travail salarié lorsqu'il existe des faits qui indiquent que le travailleur est contrôlé et dirigé par la plateforme. La définition de ces faits incombe toutefois aux Etats membres de l'UE. La directive oblige ceux-ci à prévoir des procédures adéquates et efficaces pour déterminer la qualité de travailleur. La présomption mentionnée en faveur de cette qualité peut être renversée par la plateforme, à qui il appartient alors d'apporter la preuve qu'aucun contrat de travail n'existe.

Les personnes qui travaillent via la plateforme bénéficieraient ainsi des droits liés au statut de travailleur, ce qui leur permettrait par exemple de bénéficier du salaire minimum (s'il existe), de négociations tarifaires, d'horaires de travail réglementés, d'une protection de la santé ou de congés payés. La présomption légale ne s'applique pas aux procédures liées à des questions fiscales, pénales et de sécurité sociale, contrairement à ce que la proposition de la Commission prévoyait initialement. Toutefois, les Etats membres pourront appliquer la présomption légale dans le cadre de ces procédures en vertu de leur droit national.

Les nouvelles règles prévoient en outre une série de protections en cas d'utilisation d'algorithmes par la plateforme. Elles visent notamment à garantir qu'une personne effectuant un travail sur une plateforme ne puisse pas être licenciée sur la base d'une décision prise par un algorithme ou un système décisionnel automatisé. Les plateformes doivent s'assurer que les décisions importantes qui concernent directement les personnes travaillant sur la plateforme soient supervisées par des humains.

La directive prévoit en outre des règles de protection pour les travailleurs des plateformes en matière de protection des données. Les plateformes ont l'interdiction de traiter certains types de données à caractère personnel, comme celles qui portent sur les convictions personnelles et sur les échanges privés avec les collègues.

Le texte vise également à améliorer la transparence en obligeant les plateformes à informer les travailleurs et leurs représentants sur le fonctionnement des algorithmes et sur les conséquences du comportement d'un travailleur sur les décisions prises par les systèmes automatisés.

Les plateformes doivent fournir des informations sur les travailleurs indépendants qu'elles emploient aux autorités nationales compétentes et aux représentants des travailleurs des plateformes, tels que les syndicats.

Situation actuelle

La directive est entrée en vigueur le 1er décembre 2024. Les Etats membres disposent de deux ans pour la transposer dans leurs droits nationaux respectifs.

Possibles conséquences pour la Suisse

La directive ne sera pas applicable en Suisse, mais elle pourrait avoir des conséquences dans les situations transfrontières régies par le droit d'un pays membre de l'UE. Par exemple, une plateforme en Suisse, dont la relation avec les personnes qu'elle emploie est régie par le droit étranger (c'est en général le cas si les personnes exécutent leur travail à l'étranger), pourrait être nouvellement qualifiée d'employeur, et donc soumise aux obligations qui en découlent. Les situations varieront d'un pays à l'autre, selon la manière dont les Etats transposeront la directive.

Mesures déjà prises en Suisse

Dans son rapport Numérisation – Examen d'une flexibilisation dans le droit des assurances sociales du 27 octobre 2021, le Conseil fédéral a analysé en détail le cadre légal et les différentes options d'un développement du droit des assurances sociales en relation avec les nouveaux modèles d'affaires numériques. Il a également examiné les avantages et les inconvénients d'une réglementation qui présupposerait que le travail de plateforme constituerait une activité salariée. Il est parvenu à la conclusion qu'il n'y avait pas lieu d'agir davantage à cet égard. En droit du travail, une décision du Tribunal cantonal vaudois concernant un chauffeur de la société Uber, et deux décisions du Tribunal fédéral concernant Uber et Uber Eats ont permis d'établir les critères pertinents pour qualifier de travail salarié l'activité réalisée pour une plateforme. Le Conseil fédéral n'a pas non plus jugé nécessaire de légiférer dans ce domaine, avis qu'il a dernièrement confirmée dans son rapport du 9 décembre 2022, Conséquences de la numérisation sur le marché du travail - Monitorage 2022.

Mesure 23

Stratégie blockchain européenne

Appellation complète de la mesure	Stratégie blockchain européenne
Type de mesure	Stratégie
Référence	Blockchain Strategy
Unité responsable dans l'administration fédérale	SFI

Description

En février 2020, la Commission européenne a annoncé dans sa communication "Façonner l'avenir numérique de l'Europe" l'élaboration de stratégies dans le domaine des technologies quantiques et de la blockchain. Elle utilise la terminologie Blockchain Strategy comme terme générique pour les mesures qui doivent concrétiser la volonté de l'UE de jouer un rôle de premier plan dans le domaine de la blockchain. La stratégie comprend les domaines thématiques et les initiatives suivantes :

- **Création d'une blockchain paneuropéenne pour les services publics :** Le European Blockchain Partnership, que la Commission a lancé conjointement avec les Etats membres de l'UE ainsi que les Etats de l'EEE, travaille sur l'European Blockchain Services Infrastructure (EBSI). Il s'agit d'une infrastructure blockchain commune pour les services publics. Les activités d'infrastructure (comme l'acquisition de la plateforme EBSI) sont financées par le programme Digital Europe.
- **Adaptation du cadre réglementaire :** La Commission souhaite établir des normes dans le domaine de la blockchain et créer une sécurité juridique grâce aux futures législations, notamment le règlement Market in Crypto Assets (MiCA), entré en vigueur en juin 2023 et applicable à partir du 30 décembre 2024, ainsi que du régime pilote pour les infrastructures des marchés financiers basées sur la Distributed Ledger Technology. Le règlement MiCA prévoit en outre, avant l'application du nouveau régime, une série de normes techniques à définir qui seront publiées successivement en trois paquets (voir aperçu de l'ESMA).
- **Investissement dans la recherche et l'innovation :** Horizon Europe et le Fonds d'investissement IA/Blockchain de l'UE financent des investissements dans la recherche et l'innovation.
- **Formation et soutien communautaire :** La Commission encourage l'éducation dans le domaine numérique et cherche à échanger avec les principaux acteurs de la communauté de la blockchain. Afin de suivre les évolutions de la blockchain et de promouvoir l'innovation, la Commission a créé en 2018 l'Observatoire et forum de la blockchain de l'UE.

Situation actuelle

Les travaux sont suivis dans les différents domaines thématiques et les initiatives sont lancées.

Possibles conséquences pour la Suisse

La Suisse a rapidement réglementé l'utilisation de la DLT/blockchain, avec un paquet entré en force en 2021. La nouvelle réglementation dans l'UE pourrait entrainer une concurrence plus forte pour les prestataires suisses en créant un cadre juridique pour l'utilisation de la technologie blockchain dans le secteur financier, aussi dans le contexte où MiCA ne prévoit pas d'accès au marché de l'UE par des prestataires de pays tiers (p. ex. Suisse). En même temps, un grand nombre d'experts dans l'UE se plaignent de problèmes en lien avec l'application de MiCA qui est, selon eux, mal ficelé et va conduire à beaucoup de difficultés en pratique.

Mesures déjà prises en Suisse

Le SFI suit de près les développements et évalue le cadre de l'Union européenne dans le cadre des travaux réglementaires portant sur l'utilisation de la technologie blockchain dans les marchés financiers.

Mesure 24

Loi pour une Europe interopérable

Appellation complète de la mesure	Règlement pour une Europe interopérable
Type de mesure	Règlement
Référence	Règlement 2022/0379 (COD)
Etat actuel	En vigueur
Date d'entrée en vigueur	11.04.2024
Unité responsable dans l'administration fédérale	ChF

Description

Le règlement pour une Europe interopérable (IEA) vise à faciliter l'échange transfrontière de données et à accélérer la transformation numérique du secteur public. Il doit contribuer à atteindre les objectifs de la Décennie numérique de l'UE, notamment celui d'avoir 100% des services publics clés disponibles en ligne d'ici à 2030.

La législation établit un nouveau cadre de coopération entre les Etats membres de l'UE et la Commission européenne (COM) pour un travail commun sur les questions relatives à l'interopérabilité transfrontalière et aux services publics numériques. Dans ce contexte, les Etats membres et la COM conviennent de priorités et de solutions communes en matière d'interopérabilité.

En outre, la loi impose aux institutions européennes et aux organismes et agences du secteur public de procéder à des évaluations de l'interopérabilité afin d'identifier et de prendre en compte les aspects numériques et d'interopérabilité dès la phase de conception des politiques et des services publics numériques.

La nouvelle législation facilite également le partage et la réutilisation des solutions ainsi que l'échange de données entre les administrations, en supprimant les charges administratives inutiles liées aux obstacles juridiques, organisationnels, sémantiques et techniques à l'interopérabilité. Cela permet de réduire les coûts et les délais pour les citoyens, les entreprises et le secteur public lui-même.

Le règlement s'applique aux organismes du secteur public, y compris les institutions et organes de l'UE. Sa mise en œuvre sera financée par le programme pour une Europe numérique (Digital Europe).

Situation actuelle

L'Etat actuel de l'IEA est le suivant :

1. Adoption : Le Parlement européen a adopté l'IEA le 6 février 2024.
2. Structure de gouvernance : Un Board Europe interopérable a été créé pour orienter et contrôler le cadre de coopération en matière d'interopérabilité. Le Parlement européen a plaidé pour une participation plus large des acteurs pertinents.
3. Suivi : L'IEA prévoit que la Commission rédige un rapport annuel sur le développement de solutions libres d'interopérabilité entre les logiciels destinées aux services publics.

L'IEA est entré en vigueur le 11 avril 2024. Conformément au calendrier défini dans le règlement, la plupart des dispositions s'appliquent dans les trois mois suivant la date d'entrée en vigueur.

Exceptionnellement :

- Les institutions, organes et agences européens ainsi que les organismes du secteur public procéderont à des évaluations de l'interopérabilité à partir de janvier 2025 ;
- Les Etats membres de l'UE désigneront les autorités nationales compétentes 9 mois après la date d'entrée en vigueur du règlement, soit en janvier 2025.

Possibles conséquences pour la Suisse

L'IEA s'applique aux institutions de l'Union et aux organismes publics qui réglementent, mettent à disposition, gèrent ou fournissent des services publics numériques transeuropéens. Il n'a donc pas de conséquences directes sur la Suisse.

Mesures déjà prises en Suisse

En Suisse, la LMETA et l'OMETA visant à promouvoir l'interopérabilité sont entrés en vigueur le 1er janvier 2024. Cette mesure s'inscrit dans le contexte de la numérisation de l'administration et ne constitue pas une réaction directe à la mesure de l'UE.

Mesure 25

Accès aux données financières

Appellation complète de la mesure	Règlement relatif à un cadre pour l'accès aux données financières
Type de mesure	Paquet législatif
Référence	2023/0205 (COD)
Etat actuel	Pas en vigueur
Date d'entrée en vigueur	Prévue début ou mi-2025
Unité responsable dans l'administration fédérale	SFI

Description

Le 28 juin 2023, comme prévu, la Commission européenne a présenté une proposition de règlement relatif à un cadre pour l'accès aux données financières (FiDA) dans le contexte du paquet sur l'accès aux données financières et les paiements. Ce règlement doit définir des droits et des obligations pour gérer l'échange de données clients dans le secteur financier au-delà des comptes de paiement, dans l'espoir que cela conduise à des produits et services financiers plus innovants et à une concurrence accrue dans le secteur financier. Son champ d'application comprend donc non seulement les données de paiement, mais aussi les données non bancaires, telles que les données d'assurance, d'investissement et de retraite. La proposition repose en outre sur le principe selon lequel les clients des services financiers sont propriétaires des données qu'ils fournissent et de celles qui sont créées en leur nom, et que ce sont eux qui les contrôlent.

La proposition Open Finance - via le règlement FiDA - s'appuie sur la directive Open Banking, qui devait être lancée avec la deuxième directive sur les services de paiement (PSD2), mais qui, dans la pratique, n'a pas répondu aux attentes, notamment en raison d'une adoption incohérente et de divergences dans l'infrastructure. En conséquence, la directive concernant les services de paiement a été révisée dans le même paquet que le règlement FiDA (PSD3), et rédigée sous la forme d'un règlement directement applicable (PSR). La révision a notamment pour objectif d'améliorer le fonctionnement de l'Open Banking en supprimant les obstacles existants.

Situation actuelle

FiDA:

- Le Parlement et le Conseil ont commencé à travailler sur la proposition, mais n'ont pas encore pris de position de négociation.

PSD3/PSR :

- Positions du Parlement en première lecture le 23 avril 2024 (Directive / Règlement). Certaines adaptations ont été faites, notamment au niveau des exigences en matière de transparence et de protection des clients.
- Le Conseil n'a pas encore finalisé son mandat pour les négociations interinstitutionnelles.

Possibles conséquences pour la Suisse

Les règlements FiDA et PSD3/PSR devraient renforcer la position de l'UE en matière d'innovation et de numérisation. En Suisse, il n'existe pas de réglementation similaire obligeant les institutions financières à ouvrir leurs données à des prestataires tiers sur demande des clients. Le DFF suit des objectifs fixés par le Conseil fédéral dans ce domaine. L'approche est basée sur le marché. Le Conseil fédéral a mandaté le DFF de l'informer régulièrement sur les progrès et le besoin de mesures.

Dans le cadre de la motion 22.3890 "Elaboration d'une loi-cadre sur la réutilisation des données", le Conseil fédéral est chargé de créer les bases permettant de développer et mettre en place rapidement des infrastructures spécifiques pour la réutilisation des données dans des domaines stratégiques. L'OFJ a pris connaissance de la présente mesure de l'UE au cours de ses travaux législatifs habituels, mais à ce stade il est trop tôt pour dire de quelle manière elle pourra être prise en compte et intégrée dans le projet relatif à la réutilisation des données.

Mesures déjà prises en Suisse

Actuellement, les mesure prises en Suisse sont la formulation d'objectifs, le suivi de près des progrès en Suisse et l'évaluation régulière du besoin de mesures.

Mesure 26

Subventions étrangères ayant un effet de distorsion

Appellation complète de la mesure	Règlement relatif aux subventions étrangères faussant le marché intérieur
Type de mesure	Règlement
Référence	Règlement (UE) 2022/2560
Etat actuel	En vigueur
Date d'entrée en vigueur	12.07.2023
Unité responsable dans l'administration fédérale	SECO/DFAE

Description

Le 12 juillet 2023, le Règlement (UE) 2022/2560 (règlement sur les subventions étrangères - FSR) est entré en vigueur. Ce nouvel ensemble de règles permet à la Commission européenne (COM) de "remédier aux distorsions causées par les subventions étrangères et à l'UE de garantir des conditions de concurrence équitables pour toutes les entreprises opérant dans le marché unique, tout en restant ouverte au commerce et à l'investissement".

Avant ce règlement, les subventions accordées par des gouvernements de pays tiers n'étaient pas contrôlées, alors que les subventions accordées par les Etats membres de l'UE font l'objet d'un examen minutieux en vertu des règles de l'UE relatives aux aides d'Etat :

- Il incombe à la **DG COMP** de faire respecter le règlement FSR en ce qui concerne les concentrations
- Il incombe à la **DG GROW** de faire respecter le règlement FSR en ce qui concerne les procédures de passation de marchés publics.

Dans tous les domaines, les entreprises et les secteurs sont concernés.

Situation actuelle

Le règlement FSR permet à la COM d'investiguer **(i)** si des entreprises étrangères qui acquièrent des entités dans l'UE ont été soutenues par de l'argent public et **(ii)** si des entreprises étrangères qui répondent à des appels d'offres dans l'UE ont été soutenues par de l'argent public. La COM peut en outre **(iii)** examiner de sa propre initiative des informations concernant de présumées subventions étrangères faussant le marché intérieur.

Le 26 mars 2024, l'entreprise chinoise CRRC Locomotive s'est retirée d'une procédure de passation de marché public lancée par le ministère bulgare des transports. Ce retrait fait suite à l'annonce de l'ouverture de la première enquête de la Commission au titre du FSR du 16 février 2024.

D'autres enquêtes ont par la suite été ouvertes dans le secteur des énergies renouvelables, qui concernaient toutes des entreprises chinoises. En outre, le 23 avril 2024, la COM a mené une inspection inopinée dans les locaux de l'entreprise de sécurité chinoise Nuctech (scanner de bagages), à Rotterdam et Varsovie. Le 13 mai 2024, deux consortiums chinois, l'un comprenant la filiale allemande de LONGi (Hong Kong) et l'autrem composé de deux sociétés du Shanghai Electric Group (Chine) ont annoncé se retirer de l'appel d'offre lancé par la Roumanie pour la construction et l'exploitation d'un parc solaire. La COM clôt donc son enquête ouverte le 3 avril 2024. En réaction, la Chambre de commerce chinoise auprès de l'UE a publié un communiqué dans lequel elle qualifie le règlement FSR d'"outil coercitif et discriminatoire". Elle met en garde contre "l'escalade des tendances

protectionnistes de l'UE". Le 10 Juin, la COM a ouvert une première enquête approfondie afin d'apprécier, au titre du règlement FSR, l'acquisition par Emirates Telecommunications Group Company PJSC (e&) du contrôle exclusif de PPF Telecom Group B.V, à l'exclusion de son activité tchèque. La COM craint, à titre préliminaire, que l'entreprise ait pu bénéficier de subventions étrangères susceptibles de fausser le marché intérieur de l'UE.

La COM se félicite des résultats rapides (voir le discours de M. Vestager du 9 avril 2024) produits par le règlement FSR, notamment pour les marchés publics. Après un problème de personnel, la DG COMP a créé la nouvelle direction K (chargée de l'analyse des notifications de concentrations), ce qui devrait améliorer l'efficacité de la mise en œuvre au cours des années à venir.

Possibles conséquences pour la Suisse

Les entreprises suisses qui exercent une activité économique sur le marché intérieur de l'UE doivent composer avec de nouveaux pouvoirs de la Commission en matière de contrôle et d'exécution dans l'UE, qui entraînent une augmentation de la charge administrative et une insécurité juridique.

Les entreprises doivent traiter tous les apports financiers des trois dernières années du point de vue de la législation sur les subventions, pour satisfaire aux obligations de notification potentielles et de pouvoir fournir les informations nécessaires à la demande de la Commission. Ces informations servent non seulement à déterminer si une future concentration d'entreprises ou une participation à des appels d'offres publics dans l'UE doit être notifiée, mais aussi pour le cas où la Commission ouvrirait une enquête d'office (p. ex. pour les plaintes de concurrents). La notion de "contribution financière" donnée par le règlement étant très large, elle donnera vraisemblablement lieu à des obligations de clarification et de collecte de données considérables.

Pour qu'une contribution financière constitue une subvention étrangère étatique ayant un effet de distorsion sur le marché intérieur de l'UE, elle doit améliorer la position concurrentielle de l'entreprise bénéficiaire et porter effectivement ou potentiellement préjudice à la concurrence sur le marché intérieur de l'UE. La qualification dépend du cas d'espèce, implique une pesée des effets positifs et négatifs de la subvention sur le marché intérieur de l'UE et peut conduire à des mesures correctives de grande portée. L'évaluation de la pesée laisse à la Commission une grande marge d'appréciation, source d'insécurité juridique.

Il convient toutefois de noter que, dans la pratique actuelle et selon de nombreuses déclarations de la Commission, le règlement sur les subventions aux pays tiers est principalement dirigé contre les entreprises des économies non marchandes, et donc pas contre les entreprises suisses. Par conséquent, il ne faut guère s'attendre actuellement à des enquêtes contre des entreprises suisses.

Mesures déjà prises en Suisse

La Suisse n'a pas pris de mesures propres dans ce domaine.

Mesure 27

Nouvel agenda du consommateur

Appellation complète de la mesure	Nouvel agenda du consommateur
Type de mesure	Paquet législatif
Référence	COM(2020) 696 final
Etat actuel	En vigueur
Date d'entrée en vigueur	13.11.2020
Unité responsable dans l'administration fédérale	BFC

Description

Le nouvel agenda du consommateur, qui présente une vision de la politique des consommateurs de l'UE pour la période de 2020 à 2025, a été communiqué par la Commission européenne le 13 novembre 2020. Il propose que plusieurs directives soient adaptées afin de protéger les consommateurs de manière adéquate, notamment en ce qui concerne la numérisation, la durabilité et la crise du covid-19.

Dans le domaine numérique, la Commission européenne entend intensifier la lutte contre la tromperie en ligne et la publicité cachée, et tenir compte des intérêts des consommateurs dans de l'élaboration de prescriptions sur l'intelligence artificielle. L'UE a révisé la directive sur la sécurité des produits et la directive sur les machines (reformulée en tant que règlement) afin d'adapter les prescriptions actuelles à l'évolution de la numérisation et à la multiplication des produits connectés. Afin de renforcer la protection des consommateurs face à la numérisation des services financiers de détail, les directives sur le crédit à la consommation et sur les services financiers à distance ont également été révisées. En outre, la révision des dispositions relatives à la sécurité des jouets vise, entre autres, à garantir une gestion sûre des nouveaux risques liés aux jouets connectés à internet et aux jouets impliquant l'intelligence artificielle, ainsi qu'à fournir des informations numériques sur les produits. La procédure législative liée à cette proposition est toutefois toujours en cours. Les nouvelles dispositions horizontales relatives à l'utilisation de l'IA prévues dans le cadre de l'AI Act (voir mesure 5) devraient également contribuer à la protection des consommateurs.

Dans le domaine de l'environnement, l'UE a également adopté une nouvelle directive visant à donner aux consommateurs les moyens d'agir en faveur de la transition écologique, qui devrait permettre aux consommateurs d'être mieux informés sur la durée de vie des produits et de se protéger davantage contre des pratiques telles que l'écoblanchiment et l'obsolescence programmée. La nouvelle directive sur l'étayage et la communication des allégations environnementales explicites (Green Claims Directive), encore en cours de procédure législative, poursuit des objectifs similaires.

La révision de la directive sur le commerce des biens encourage également la réparation et les produits plus durables. Les nouvelles dispositions visant à promouvoir la réparation des biens, publiées au Journal officiel le 10 juillet 2024 après leur adoption par les co-législateurs, poursuivent elles aussi cet objectif.

Enfin, une protection adéquate des consommateurs passe également par une bonne coopération au sein de l'UE et avec les partenaires internationaux. La Commission européenne souhaite renforcer la coopération internationale, notamment avec la Chine, afin de tenir compte de l'émergence du commerce en ligne.

Situation actuelle

Le 13 novembre 2020, la Commission européenne a adopté le nouvel agenda du consommateur, qui constitue une mise à jour du cadre stratégique global de la politique de protection des consommateurs de l'UE, initialement adopté en 2012.

Possibles conséquences pour la Suisse

L'agenda du consommateur comprend une vision et un plan d'action pour la politique des consommateurs de l'UE et n'a donc pas de conséquences directes pour la Suisse. Il n'existe actuellement aucun accord qui oblige la Suisse à reprendre la législation européenne en matière de protection des consommateurs, à l'exception de l'accord bilatéral sur le transport aérien (en vertu duquel la Suisse a notamment repris le règlement UE/261/2004 en matière d'indemnisation et d'assistance des passagers en cas de refus d'embarquement et d'annulation ou de retard important d'un vol) et de l'accord bilatéral sur les transports terrestres (en vertu duquel la Suisse a notamment repris le règlement (CE) 1371/2007 sur les droits et obligations des voyageurs ferroviaires et le règlement (UE) 181/2011 concernant les droits des passagers dans le transport par autobus et autocar).

Dans l'Agenda, la Commission européenne souligne à plusieurs reprises l'importance de la coopération entre les autorités pour garantir un niveau élevé de protection des consommateurs. Le règlement EU/2017/2394, qui régit la coopération entre les autorités de l'UE, prévoit la possibilité de conclure des accords avec des pays tiers.

Mesures déjà prises en Suisse

La Suisse a reproduit de manière autonome les règles de protection des consommateurs, notamment dans les domaines suivants : voyages à forfait, responsabilité du fait des produits, démarchage à domicile, crédit à la consommation, pratiques commerciales déloyales et sécurité des produits. La législation suisse et la législation européenne présentent toutefois certaines différences en matière de protection des consommateurs. Des adaptations de la législation suisse concernant les voyages à forfait, la vente de biens, les contrats portant sur des biens et services numériques, les pratiques commerciales déloyales et la sécurité des produits sont actuellement en cours de discussion ou d'examen. Par contre, dans un rapport du 16 juin 2023 intitulé "Modernisation du droit de la garantie", le Conseil fédéral a estimé qu’il n’était pas nécessaire de légiférer sur l'obsolescence programmée, et que le problème pouvait se résoudre sur la base des règles générales en vigueur.

Mesure 28

Plan d’action pour la démocratie européenne

Appellation complète de la mesure	Plan d'action pour la démocratie européenne
Type de mesure	Plan d’action
Référence	Plan d’action pour la démocratie européenne
Etat actuel	-
Date d’entrée en vigueur	-
Unité responsable dans l’administration fédérale	OFCOM/ChF

Description

La Commission européenne (COM) entend garantir que les progrès envisagés dans le cadre de la "décennie numérique de l’Europe" n’altéreront pas davantage le **respect de la démocratie et des droits fondamentaux** dans l’UE. Pour cela, la COM a adopté en décembre 2020 un "garde-fou" sous la forme d’un Plan d’action européen pour la démocratie (European Democracy Action Plan, [EDAP]). Ce dernier devrait apporter une réponse aux nouveaux défis engendrés par la révolution numérique tels que les interférences récurrentes dans les processus démocratiques, les menaces qui pèsent sur les journalistes ou encore le manque de transparence des géants du numérique.

La COM prévoit des mesures visant à **1) promouvoir des élections libres et régulières, 2) soutenir la liberté et l'indépendance des médias et 3) lutter contre la désinformation**. Le plan mentionne le cadre complémentaire offert par la législation sur les services numériques, qui permettra la surveillance, la responsabilité et la transparence, ainsi que la mise en place d'un **soutien de co-régulation avec le Code de bonnes pratiques renforcé sur la désinformation**.

Les initiatives prévues par l'EDAP (en particulier celles qui concernent le renforcement du code de conduite et la régulation sur la transparence pour la publicité politique) complètent les mesures proposées dans le cadre de la législation sur les services numériques (DSA).

Concrètement, en application de ce plan d'action, la COM a publié, en septembre 2021, une recommandation visant à renforcer la sécurité des journalistes et autres professionnels des médias, à la fois en ligne et hors ligne. Des mesures sont également envisagées pour promouvoir la diversité des médias et accroître la transparence des rapports de propriété dans le secteur. A cet égard, depuis mai 2024, l’UE dispose d’une législation européenne sur la liberté des médias, qui propose un nouvel ensemble de règles visant à protéger le pluralisme et l’indépendance des médias dans de l’UE (voir également la mesure 29). Par ailleurs, depuis 2024, une nouvelle directive destinée à améliorer la protection des journalistes et des défenseurs des droits de l'homme contre les procédures judiciaires abusives (SLAPP) couvre les poursuites judiciaires dans les affaires civiles ayant des implications transfrontalières.

Situation actuelle

En 2023, avant les élections européennes, la COM a examiné la mise en œuvre du plan d'action et identifié un certain nombre de domaines dans lesquels l'UE peut être proactive face aux défis existants et en évolution. Elle a présenté une recommandation relative à des processus électoraux inclusifs et résilients dans l’UE, au renforcement du caractère européen des élections au Parlement européen et à une meilleure garantie de leur bon déroulement, une proposition pour une directive en matière de transparence de la représentation d’intérêts

exercée pour le compte de pays tiers, ainsi qu'une recommandation relative à la promotion de l'implication des citoyens et des organisations de la société civile dans les processus d'élaboration des politiques publiques, et de leur participation effective à ces processus.

Possibles conséquences pour la Suisse

Le plan d'action pour la démocratie concerne également la Suisse, notamment sur les activités liées à la résilience des processus électoraux, à la lutte contre la désinformation et à la transparence des représentants d'intérêts issus de pays tiers.

Jusqu'à présent, la Suisse n'est pas impliquée dans le réseau européen de coopération électorale, mis en place en 2019. Compte tenu des projets concrets d'échange au sein de ce réseau, en particulier sur les questions d'intégrité des élections (comme la cybersécurité des élections), il serait avantageux pour elle de se voir associée plus étroitement aux travaux.

Dans son rapport sur la politique de sécurité, le Conseil fédéral indique que les activités d'influence et la désinformation doivent être combattues par le renforcement de la détection précoce, du suivi de la situation et de la résilience de la population suisse, ainsi que par une communication active des autorités. En réponse au Po. 22.3006 CPS-N, le 19 juin 2024, il a adopté le rapport Activités d'influence et désinformation. Il y expose en quoi la Suisse est concernée par les activités d'influence menées dans l'espace d'information, quelles sont les caractéristiques pertinentes de la Suisse et quelles mesures supplémentaires il entend prendre pour faire face à ces menaces. Dans ce contexte, la Suisse gagnerait à s'intégrer davantage dans les structures de coopération de l'UE, notamment le système d'alerte rapide (Rapid Alert System, RAS).

Selon le projet de directive, l'obligation de transparence s'appliquerait aux représentants d'intérêts issus de pays tiers, et donc aussi aux acteurs suisses, mais pas à ceux des Etats de l'UE ni de l'EEE. Par ailleurs, les Etats de l'UE et de l'EEE seraient tenus d'exploiter un registre national de transparence. Certaines questions restent ouvertes quant à la forme concrète de la directive, raison pour laquelle une évaluation définitive des conséquences pour la Suisse n'est pas encore possible.

Mesures déjà prises en Suisse

S'agissant de la transparence du financement de la politique, la législation fédérale a été adaptée. Les nouvelles dispositions, entrées en vigueur le 23 octobre 2022, ont été appliquées pour la première fois à l'occasion des élections au Conseil national de 2023. L'évolution de la réglementation européenne n'a pas de conséquences directes sur la Suisse, mais elle doit être suivie, en vue d'éventuelles modifications de la législation. La Suisse ne dispose actuellement d'aucune loi ou règle spécifique pour lutter contre la désinformation. En revanche, le 19 juin 2024, en même temps qu'il adoptait le rapport "Activités d'influence et désinformation", le Conseil fédéral a décidé de prendre des mesures supplémentaires pour faire face aux menaces dans l'espace d'information.

Mesure 29

Règlement européen sur la liberté des médias

Appellation complète de la mesure	Règlement établissant un cadre commun pour les services de médias dans le marché intérieur
Type de mesure	Règlement
Référence	Règlement 2024/1083
Etat actuel	En vigueur
Date d'entrée en vigueur	07.05.2024
Unité responsable dans l'administration fédérale	OFCOM

Description

Le règlement pour la liberté des médias vise à renforcer l'intégrité du marché intérieur et à protéger ainsi le pluralisme et l'indépendance des médias dans l'Union. La législation poursuit les objectifs suivants :

- Protéger l'indépendance éditoriale en exigeant des Etats membres qu'ils respectent la liberté éditoriale effective des fournisseurs de services de médias ;
- Protéger les sources journalistiques, y compris contre l'utilisation de logiciels espions ;
- Garantir le fonctionnement indépendant des médias de service public, notamment en garantissant des ressources financières adéquates, durables et prévisibles, et en favorisant la transparence dans la nomination du chef ou des membres des conseils d'administration des médias de service public ;
- Garantir la transparence de la propriété des médias en exigeant que les fournisseurs de services de médias divulguent des informations spécifiques qui les concernent (p. ex. noms légaux, coordonnées, propriété) ;
- Prévoir des garanties contre le retrait injustifié par les très grandes plateformes en ligne (désignées en vertu de la législation sur les services numériques) de contenus médiatiques produits selon des normes professionnelles, mais jugés incompatibles avec les conditions générales ;
- Introduire un droit de personnalisation de l'offre multimédia sur les appareils et interfaces, tels que les téléviseurs connectés, qui permette aux utilisateurs de modifier les paramètres par défaut pour refléter leurs propres préférences ;
- Veiller à ce que les Etats membres fournissent une évaluation de l'incidence qu'ont les principales concentrations de médias sur le pluralisme des médias et sur l'indépendance éditoriale, évaluation qu'ils doivent mener au moyen de tests de pluralisme des médias ;
- Garantir une plus grande transparence en matière de mesure de l'audience pour les fournisseurs de services de médias et les annonceurs, afin de limiter le risque de données gonflées ou biaisées ;
- Etablir des exigences de transparence pour l'attribution, par les autorités et entités publiques, de la publicité d'Etat aux fournisseurs de services de médias et aux plateformes en ligne ;
- Intensifier et étendre la coopération et la coordination entre les régulateurs des médias, y compris en ce qui concerne les mesures relatives aux services de médias provenant de l'extérieur de l'Union.

La législation instaure un nouveau comité européen pour les services de médias, instance indépendante composée d'autorités nationales chargées des médias, qui va dissoudre et remplacer le Groupe des régulateurs européens des services de médias audiovisuels (ERGA). Le comité encouragera l'application efficace et cohérente du cadre législatif de l'UE sur les médias, notamment en assistant la COM dans l'élaboration de lignes directrices concernant la réglementation des médias. Il pourra également émettre des avis à propos des mesures et décisions nationales ainsi que des concentrations des médias qui influencent le marché.

Situation actuelle

La législation est entrée en vigueur le 7 mai 2024 et sera applicable dès le 8 août 2025, à quelques exceptions. La mise en place du comité européen pour les services des médias sera ainsi déjà effectuée à partir du 8 février 2025.

Possibles conséquences pour la Suisse

Il est encore trop tôt pour savoir quelles conséquences cette réglementation aura pour la Suisse. La première mesure qui la concernera sera la mise en place du comité européen pour les services des médias, et il n’est pas certain que le statut d’observateur au sein de l’ERGA dont elle bénéficie actuellement reste garanti dans le nouveau comité.

Mesures déjà prises en Suisse

La Suisse n'a pas pris de mesures propres dans ce domaine.

Mesure 30

Stratégie de normalisation

Appellation complète de la mesure	Stratégie en matière de normalisation
Type de mesure	Stratégie
Référence	Stratégie COM (2022) 31
Etat actuel	Publiée
Date d'entrée en vigueur	02.02.2022
Unité responsable dans l'administration fédérale	SECO

Description

Le 2 février 2022, après plusieurs reports, la Commission européenne a publié une nouvelle stratégie de normalisation, qui vise à renforcer la compétitivité mondiale de l'UE, à permettre le passage à une économie résiliente, verte et numérique et à ancrer les valeurs démocratiques dans les applications technologiques. L'UE considère que dans la course mondiale à la primauté numérique, il est essentiel pour sa compétitivité qu'elle soit en mesure de définir des normes internationales qui constituent des références mondiales pour les produits, processus et services numériques. La stratégie prévoit cinq séries de mesures : 1) anticiper, hiérarchiser et gérer les besoins de normalisation dans des domaines stratégiques ; 2) améliorer la gouvernance et l'intégrité du système européen de normalisation ; 3) renforcer le rôle moteur de l'Europe en matière de normes mondiales ; 4) encourager l'innovation et 5) faciliter le renouvellement des générations d'experts. Le règlement 1025/2012 sur la normalisation a également été modifié pour correspondre à la stratégie. Il a été publié au Journal officiel le 19 décembre 2022 et est entré en vigueur 20 jours plus tard.

Dans le cadre de la stratégie de normalisation, la COM a institué le groupe d'experts "Forum de haut niveau sur la normalisation européenne". Ce forum a pour tâche de contribuer à :

- L'identification et la mise en œuvre de priorités annuelles pour la normalisation européenne dans le but de soutenir un marché unique vert, numérique, équitable et résilient ;
- L'identification d'éventuels besoins futurs en matière de normalisation dans le but de soutenir la législation, des programmes et des politiques de l'Union.

Il a également pour tâche de conseiller la COM sur :

- Les questions liées à la politique européenne de normalisation ;
- La coordination de la représentation efficace des intérêts de l'UE auprès des organisations et organismes internationaux de normalisation ;
- Les moyens d'assurer des activités européennes de normalisation adaptées aux besoins, en vue de rendre l'économie de l'Union plus verte, plus numérique, plus équitable et plus résiliente ;
- Les moyens de mieux associer les activités de recherche, de développement et d'innovation, de renforcer l'enseignement supérieur ainsi que l'expertise et les compétences en matière de normalisation.

Parallèlement, la Commission européenne élabore et met à jour, chaque année, le plan glissant de normalisation des TIC, en collaboration avec la plateforme européenne multipartite de normalisation des TIC. Le document recense tous les thèmes identifiés comme étant des priorités politiques de l'UE et pour lesquels la normalisation, les normes ou les spécifications techniques liées aux TIC devraient jouer un rôle clé dans la mise en œuvre de la politique. Il couvre les technologies d'"importance horizontale", dont l'application dans le contexte des infrastructures des TIC et de la normalisation des TIC a des conséquences majeures sur différents domaines techniques.

L'arrêt publié le 5 mars 2024 dans l'affaire C588/21 P (affaire Malamud) et qui portait sur l'accès du public aux normes européennes harmonisées – à savoir aux normes élaborées par les organismes de normalisation à la demande de la Commission et en soutien aux mesures législatives européennes –, joue également un rôle important pour la stratégie de normalisation de l'UE. Il était attendu avec beaucoup d'intérêt en raison de ses implications possibles pour les processus de normalisation. La Cour de justice de l'Union européenne (CJUE) a jugé que les normes harmonisées restaient protégées par le droit d'auteur, mais elle a annulé la décision de la

Commission de refuser l'accès aux normes pertinentes en l'espèce. Les acteurs européens sont toujours en train d'évaluer les conséquences de cet arrêt sur le système de normalisation dans son ensemble.

Situation actuelle

Le 2 février 2022, la Commission européenne a publié sa stratégie de normalisation, dans laquelle elle expose son approche des normes à l'intérieur du marché unique et à l'échelle mondiale.

Possibles conséquences pour la Suisse

La Suisse est concernée par la stratégie puisqu'elle participe autant que possible au système européen de normalisation (voir ci-après), qu'elle cofinance via l'AELE. Par contre, elle n'est pas soumise au règlement européen sur les normes 1025/2012, et ne peut donc pas être directement impliquée dans les processus qui en découlent.

Les normes internationales, en particulier les normes européennes harmonisées, ont également une grande importance pour la Suisse, qui aligne ses exigences légales relatives aux produits sur les prescriptions de l'UE (conformément à la loi fédérale sur les entraves techniques au commerce [LETC ; RS 946.51]). Dans le système dit de "nouvelle approche" adopté par l'UE, le droit européen ne définit toutefois plus que les exigences de base. Pour les produits, celles-ci sont concrétisées uniquement par des normes européennes harmonisées. Pour que les exigences essentielles ne soient pas les seules à s'appliquer en Suisse, mais qu'elles soient également concrétisées,, la Suisse transpose en général les normes européennes harmonisées telles quelles dans son système national de normalisation.

La Suisse participe à l'European Multistakeholder Platform on ICT Standardisation (MSP). Cette plateforme d'échange d'informations entre la COM, les Etats membres, la communauté de normalisation et la société civile élabore, entre autres avec la COM, le "Plan glissant de l'UE" pour la normalisation dans le secteur des TIC. La Suisse participe également en tant qu'observatrice au Comité de normalisation institué par le Règlement (UE) 1025/2012 de l'UE.

La Suisse est aussi membre des organisations européennes de normalisation, notamment le CEN, le CENELEC et l'ETSI. En 2022, à la faveur d'une révision mineure du Règlement (UE) 1025/2012 dans le cadre de la stratégie de normalisation de l'UE, elle est devenue membre de la catégorie "rouge" de ces organisations, à savoir qu'elle dispose d'un accès complet à tous les comités et groupes de travail. Toutefois, si un vote est serré, sa voix n'est plus considérée au deuxième décompte. Elle peut donc participer à l'élaboration des normes, mais elle ne peut plus participer à l'adoption ou au rejet de la norme par l'organisme de normalisation. A noter toutefois que cette pondération des voix était déjà possible avant la révision du règlement (UE) 1025/2012.

La Suisse participe au "Forum de haut niveau sur la normalisation européenne" via l'AELE, également à titre d'observatrice. Selon la Stratégie Suisse numérique, certaines technologies et certains champs d'application (planification et construction immobilières, ville intelligente, intelligence artificielle, etc.) sont prioritaires et pourraient donc bénéficier de la normalisation. Ils figurent en partie également dans la stratégie européenne en matière de normalisation (voir Plan glissant de normalisation pour les TIC).

En outre, dans sa séance du 31 août 2022, le Conseil fédéral a pris connaissance d'un rapport consacré au soutien apporté aux organismes de normalisation dans le domaine de la numérisation et qui fournit des connaissances utiles pour le soutien aux efforts de normalisation technique en Suisse. Cette étape est déterminante pour que les intérêts de la Suisse soient représentés de manière coordonnée dans les organisations de normalisation européennes et internationales.

Mesures déjà prises en Suisse

De leur propre initiative, l'Association suisse de normalisation (SNV) et l'Institut fédéral de métrologie (METAS) ont lancé un état des lieux qui devra permettre à toutes les personnes impliquées dans l'infrastructure de la qualité en Suisse d'examiner où la numérisation pourrait engendrer des effets de synergie. La démarche porte non seulement sur la normalisation, mais aussi sur l'accréditation et la métrologie légale.

De sa propre initiative, le directeur de la SNV s'est porté candidat et a été élu par l'assemblée générale au Conseil d'administration de CEN pour la période 2024-2025. Cette nomination constitue une possibilité d'extension des activités de la Suisse dans les organisations de normalisation au niveau européen et international. Une

représentation de la Suisse dans ces organes doit permettre de donner des impulsions pour renforcer la défense de ses intérêts.

Mesure 31

Stratégie sur le web 4.0 et les modes virtuels

Appellation complète de la mesure	Stratégie sur le web 4.0 et les mondes virtuels
Type de mesure	Stratégie
Référence	Stratégie sur le web 4.0 et les mondes virtuels
Etat actuel	-
Date d'entrée en vigueur	-
Unité responsable dans l'administration fédérale	OFCOM

Description

Le 11 juillet 2023, la Commission européenne (COM) a adopté une stratégie sur le web 4.0 et les mondes virtuels. Cette stratégie vise à aider l'UE à saisir les opportunités offertes par la prochaine génération du World Wide Web, tout en garantissant un environnement numérique ouvert, sûr et équitable pour les citoyens et les entreprises. Elle s'appuie sur les travaux de la Commission européenne sur les mondes virtuels et les consultations avec les citoyens, les universités et les entreprises. 23 recommandations élaborées en avril 2023 dans le cadre d'un panel de citoyens européens sur les mondes virtuels orientent les actions prévues dans la stratégie pour le web 4.0 et les mondes virtuels.

La stratégie repose sur quatre piliers :

- **Renforcer l'autonomie et les compétences des personnes :** Pour favoriser l'acceptation des évolutions technologiques et permettre à tous de participer, il convient de sensibiliser la population et de renforcer ses compétences numériques. La Commission souhaite notamment mettre en place un pool en ligne de spécialistes du monde virtuel afin que les citoyens puissent accéder à des informations sûres et fiables. Des programmes tels que Digitale Europe ou Creative Europe doivent permettre de soutenir des projets de développement des compétences pour des groupes cibles tels que les femmes et les jeunes filles ou les créateurs artistiques.
- **Entreprises :** Un écosystème industriel européen web 4.0 doit être encouragé. D'ici le premier trimestre 2024, la Commission entend étudier la mise en place d'un nouveau partenariat européen dans le but d'établir une feuille de route industrielle et technologique. Les industries culturelles et créatives seront soutenues dans le cadre de Creative Europe pour tester de nouveaux modèles commerciaux dans les mondes virtuels.
- **Pouvoirs publics :** Les mondes virtuels devraient contribuer à l'amélioration de secteurs tels que la santé et les services publics. La Commission soutiendra deux initiatives menées dans le cadre des programmes Horizon Europe et Digital Europe, à savoir CitiVerse, un environnement urbain immersif qui peut être utilisé pour la planification et la gestion urbaines, et un jumeau virtuel européen de l'homme, qui reproduit le corps humain afin de soutenir la prise de décision clinique et le traitement personnalisé.
- **Gouvernance :** Il convient de promouvoir, en collaboration avec les acteurs de la gouvernance d'internet dans le monde entier, des normes pour des mondes virtuels ouverts et interopérables et pour le web 4.0, afin de s'assurer qu'ils ne sont pas dominés par quelques grands acteurs.

Situation actuelle

La stratégie se trouve actuellement en phase de mise en œuvre

Possibles conséquences pour la Suisse

Actuellement, il n'y a pas de conséquences à attendre pour la Suisse.

Mesures déjà prises en Suisse

La Suisse n'a pas pris de mesures propres dans ce domaine.